引例 S02P0444W000

世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 G11B 20/10	A1	(11) 国際公開番号	WO00/52690
		(43) 国際公開日	2000年9月8日(08.09.00)

(21) 国際出願番号 PCT/JP99/00929

(22) 国際出願日 1999年2月26日(26.02.99)

(71) 出願人（米国を除くすべての指定国について）
株式会社 日立製作所(HITACHI, LTD.)[JP/JP]
〒101-8010 東京都千代田区神田駿河台四丁目6番地
Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
佐々本学(SASAMOTO, Manabu)[JP/JP]
相川 慎(AIKAWA, Makoto)[JP/JP]
岡本宏夫(OKAMOTO, Hiroo)[JP/JP]
野口敬治(NOGUCHI, Takaharu)[JP/JP]
〒244-0817 神奈川県横浜市戸塚区吉田町292番地
株式会社 日立製作所 マルチメディアシステム開発本部内
Kanagawa, (JP)
(74) 代理人
弁理士 作田康夫(SAKUTA, Yasuo)
〒100-8220 東京都千代田区丸の内一丁目5番1号
株式会社 日立製作所内 Tokyo, (JP)

(81) 指定国 BR, CA, CN, IN, JP, KR, SG, US, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE)

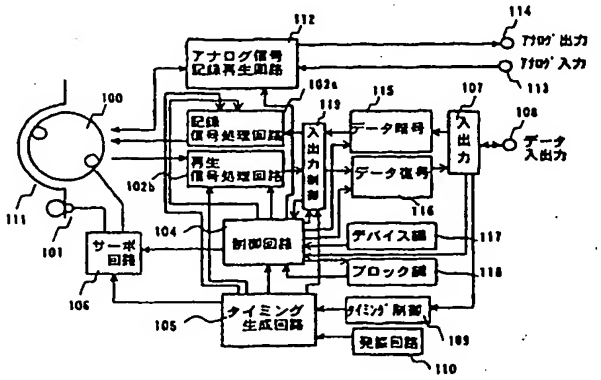
添付公開書類
国際調査報告書

(54)Title: DIGITAL SIGNAL RECORDER, REPRODUCER AND RECORDING MEDIUM

(54)発明の名称 ディジタル信号記録装置、再生装置、および記録媒体

(57) Abstract

A recorder, a reproducer and a recording medium capable of protecting a copy right of a digital signal on a recording medium; specifically a digital signal recorder, a reproducer and a recording medium for recording or reproducing a digital signal onto or from a recording medium, wherein, at recording, a digital signal is encoded by a key obtained by performing a preset calculation on a key information and is recorded on a recording medium along with the key information, and at reproducing, a reproduced digital signal is decoded by the key reproduced from the recording medium and obtained by performing the preset calculation on the key information and is output.



102a ... RECORDING SIGNAL PROCESSING CIRCUIT
102b ... REPRODUCING SIGNAL PROCESSING CIRCUIT
104 ... CONTROL CIRCUIT
105 ... TIMING GENERATION CIRCUIT
106 ... SERVO CIRCUIT
107 ... INPUT/OUTPUT
108 ... DATA INPUT/OUTPUT
109 ... TIMING CONTROL
110 ... OSCILLATION CIRCUIT
112 ... ANALOG SIGNAL RECORDING/REPRODUCING CIRCUIT
113 ... ANALOG INPUT
114 ... ANALOG OUTPUT
115 ... DATA ENCODING
116 ... DATA DECODING
117 ... DEVICE KEY
118 ... BLOCK KEY
119 ... INPUT/OUTPUT CONTROL

(57)要約

記録媒体上のディジタル信号の著作権を保護できる記録装置、再生装置、および記録媒体である。

ディジタル信号を、記録媒体上に記録または再生するディジタル信号記録装置、再生装置、および記録媒体において、記録時には、鍵情報に所定の演算を施して得られた鍵で、ディジタル信号を暗号化して、前記鍵情報とともに、記録媒体に記録し、再生時には、記録媒体から再生した前記鍵情報に、前記所定の演算を施して得られた鍵で、再生したディジタル信号を復号化して出力する。

明 細 書

ディジタル信号記録装置、再生装置、および記録媒体

技術分野

本発明は、ディジタル信号を記録媒体に記録再生するディジタル信号記録装置、再生装置、および記録媒体に関し、特に記録媒体上のディジタル信号の著作権を保護する機能を有する記録、再生装置、および記録媒体に関する。

背景技術

近年、ディジタル技術を用いた映像、音声等のデータ圧縮の研究が進み、これらデータの蓄積、伝送が容易にできるようになった。これに伴い、放送の分野においてもディジタル化が急速に進められている。

例えば、アナログ映像信号、音声信号をＭＰＥＧ（Moving Picture Experts Group）規格を用いて高能率にディジタル圧縮符号化し、衛星や同軸ケーブルを通して放送するシステムが知られている。このディジタル放送を受信するための装置として、セットトップボックスと呼ばれるディジタル放送受信機がある。

また、家庭用の映像信号、音声信号記録再生機器としては、磁気テープを用い、ディジタルＴＶ放送などのディジタル圧縮符号化された映像信号及び音声信号をディジタル信号のまま記録し再生できるディジタルＶＴＲの開発が進められている。

このディジタル放送受信機とディジタルＶＴＲは、ディジタルインターフェースで接続され、受信したディジタル放送を高品質で保存可能となる。

複数の情報が多重されて伝送されてくるディジタル信号を受信して所望の番組を選択する技術が、日本特開平８－５６３５０号に述べられている。また、回転磁気ヘッドを用いたディジタルＶＴＲについては、例えば、日本特開平５－１７４４９６号に記載されている。

さらに、ディジタル放送受信機とディジタルＶＴＲをディジタルインターフェースで接続したディジタル放送記録システムについて、アイイーイーイー　トランザクションス　オン　コンシューマー　エレクトロニクス、第４２巻３号、１９９６年８月、６１７～６２２頁（IEEE Transactions on Consumer Electronics, Vol. 42, No. 3, August 1996, p617～622「Newly Developed D-VHS Digital Tape Recording System for the Multimedia Era」）に詳しく述べらている。

しかしながら、ディジタル放送等をディジタルＶＴＲ等で記録した、記録媒体上のディジタル信号の著作権の防衛については何ら考慮されていない。

本発明の目的は、記録媒体上のディジタル信号の著作権を保護することにある。

発明の開示

本発明は、ディジタル信号を、記録媒体上に記録または再生するディジタル信号記録装置、再生装置および記録媒体において、記録時には、鍵情報に所定の演算を施して得られた鍵で、ディジタル信号を暗号化して、前記鍵情報とともに、記録媒体に記録し、再生時には、記録媒体から再生した前記鍵情報に、前記所定の演算を施して得られた鍵で、再生したディジタル信号を復号化して出力する。

図面の簡単な説明

第１図は本発明の実施例で、ディジタル放送受信機とディジタル信号記録再生装置を含む構成図である。

第２図は第１図のディジタル信号記録再生装置２００の構成図である。

第３図はディジタル映像圧縮信号のパケットの構成図である。

第４図は第３図のパケットヘッダ３０６の構成図である。

第５図はディジタル放送の伝送信号及び伝送信号より選択された信号の構成図である。

第６図は第２図のデータ暗号回路１１５の構成図である。

第７図は第６図の暗号器１１５５の構成図である。

第８図は第２図のデータ暗号回路１１５、データ復号回路１１６に供給するデータ鍵の生成例を示すところの制御回路１０４内のデータ鍵の生成図である。

第９図はテープ１１１の１トラックの記録パターンを示す図である。

第１０図は第９図のデータ記録領域７のブロックの構成図である。

第１１図は第１０図のＩＤ情報２１の構成図である。

第１２図は第９図のデータ記録領域７の１トラック分のデータの構成図である。

第１３図は１８８バイトのパケット形式で伝送されたディジタル圧縮映像信号を、第１２図のデータ４１に記録する時の１パケットのブロックの構成図である。

第１４図は第１２図のデータ記録領域７のヘッダ４４の構成図である。

第１５図は第１４図の付加情報４７の領域に、ブロック鍵を格納する場合のパックデータの構成図である。

第１６図はブロック鍵の格納方法を示す図である。

第１７図はブロック鍵の他の格納方法を示す図である。

第１８図は第１３図の時間情報２５の具体的構成図である。

第１９図は第２図のデータ復号回路１１６の構成図である。

第２０図は第２図の記録信号処理回路１０２ａおよび再生信号処理回路１０２ｂからなるディジタル記録再生信号処理回路１０２の構成図である。

第２１図はデータ記録開始時における信号処理のタイミングを示す図である。

第２２図は第２図のテープ１１１上の鍵情報を示す図である。

第２３図はデータ再生時における信号処理のタイミングを示す図である。

第２４図は第１図のディジタル信号記録再生装置２００の他の構成図である。

発明を実施するための最良の形態

以下、本発明の実施例を図面を用いて説明する。

第１図はディジタル放送受信機とディジタル信号記録再生装置を含む構成図である。２００はディジタル信号記録再生装置、２０１はディジタル放送受信装置、２０２はアンテナ、２０７は受像機である。また、２０３はチューナ、２０４は選択回路、２０５は復号回路、２０６はインターフェース回路、２０８はディジタル放送受信機２０１の動作の制御を行う制御回路である。ここで、ディジタル放送受信機２０１とディジタル信号記録再生装置２００は別体の構成で表示されているが、一体の構成となっていてもよい。

第２図は第１図のディジタル信号記録再生装置２００の構成図である。図２は記録再生兼用の装置であるが、記録と再生が独立していても同様である。１００は回転ヘッド、１０１はキャプスタン、１０２ａは記録時の記録信号の生成等を行う記録信号処理回路、１０２ｂは再生時の再

生信号の復調等を行う再生信号処理回路、１０４は記録再生モード等の制御を行う、例えば、マイクロプロセッサのような制御回路、１０５は回転ヘッド１００の回転等の基準となるタイミング信号を生成するタイミング生成回路、１０６は回転ヘッド及びテープの送り速度を制御するサーボ回路、１０７は記録信号の入力または再生信号の出力を行う入出力回路、１０９は記録時のタイミングを制御するタイミング制御回路、１１０は基準クロックを生成する発振回路、１１１はテープ、１１２はアナログ映像信号の記録再生回路、１１５はディジタル信号記録時のデータ暗号回路、１１６はディジタル信号再生時のデータ復号回路、１１７は、ディジタル情報を暗号あるいは復号する際にデータ暗号回路１１５あるいはデータ復号回路１１６に供給するデータ鍵のもとであるデバイス鍵を発生するデバイス鍵発生器、１１８はディジタル情報を暗号あるいは復号する際のデータ鍵のもう一つのもとであるブロック鍵を発生するブロック鍵発生器、１１９は記録時のパケットデータへのタイムスタンプ処理、再生時のパケットデータの出力制御を行う入出力制御回路である。

ディジタル映像圧縮信号は、パケット形式のデータで、複数チャンネルの信号が時分割多重されて伝送される。図１において、アンテナ２０２で受信されたディジタル放送信号は、チューナ２０３で復調され、その後、選択回路２０４で必要なディジタル圧縮映像信号が選択される。選択されたディジタル圧縮映像信号は、復号回路２０５で通常の映像信号に復号されて、受像機２０７に出力される。また、受信信号にスクランブル等の処理が行われているときは、選択回路２０４においてそれを解除した後に、復号処理が行なわれる。受信したディジタル放送信号の記録を行うときは、選択回路２０４において記録するディジタル圧縮映像信号及びそれに関連した情報が選択され、インターフェース回路２０

６を介してディジタル信号記録再生装置２００の入出力端子１０８より、ディジタル信号記録装置２００に入力され、記録される。また、記録したディジタル放送信号の再生を行うときは、ディジタル信号記録再生装置２００で再生されたディジタル圧縮映像信号等が、入出力端子１０８よりインターフェース回路２０６に出力される。インターフェース回路２０６に入力されたディジタル圧縮映像信号等は、選択回路２０４、復号回路２０５により、通常の受信時と同様の処理を行って、受像機２０７に出力する。

第１図のディジタル信号記録再生装置２００の構成を示す第２図において、記録時には、入出力端子１０８より入力されたパケットデータの一部が、入出力回路１０７を介して制御回路１０４に入力される。制御回路１０４では、パケットデータに付加されている情報あるいはパケットデータとは別に送られてきた情報によりパケットデータの種類等を検出し、検出結果によって記録モードを判断し、記録信号処理回路１０２ａ及びサーボ回路１０６の動作モードを設定する。次に入出力回路１０７は、記録するパケットデータをデータ暗号回路１１５に出力する。データ暗号回路１１５では、デバイス鍵発生器１１７およびブロック鍵発生器１１８により発生される鍵をもとに制御回路１０４において生成されるデータ鍵によって、入力されたパケットデータを暗号化し、これを入出力制御回路１１９に出力する。入出力制御回路１１９では、タイミング生成回路１０５からの時間情報をもとに、入力されたパケットデータにタイムスタンプを施し、これを記録信号処理回路１０２ａに出力する。記録信号処理回路１０２ａでは、制御回路１０４で判断された記録モードに応じて、誤り訂正符号、ＩＤ情報、サブコード、暗号化に使用したブロック鍵情報等を含む記録データの生成を行い且つ記録信号を生成して、回転ヘッド１００によりテープ１１１に記録する。

再生時には、まず任意の再生モードで再生動作を行い、再生信号処理回路１０２ｂでＩＤ情報を検出する。そして、制御回路１０４でどのモードで記録されたかを判断し、再生信号処理回路１０２ｂ及びサーボ回路１０６の動作モードを再設定して再生を行う。再生信号処理回路１０２ｂでは、回転ヘッド１００より再生された再生信号より、同期信号の検出、誤り検出訂正、ブロック鍵情報等の取得を行い、パケットデータを再生して入出力制御回路１１９に出力する。入出力制御回路１１９では、タイミング生成回路１０５で生成されたタイミングを基準としてタイムスタンプを取り除いたパケットデータをデータ復号回路１１６に出力する。データ復号回路１１６では、デバイス鍵発生器１１７により発生される鍵、および再生によって得られたブロック鍵をもとに、制御回路１０４において生成されるデータ鍵によって復号して、入出力回路１０７に出力する。

記録時には、入出力端子１０８より入力された記録データのレートを基準としてタイミング制御回路１０９により記録再生装置の動作タイミングを制御し、再生時には、発振回路１１０により発振されたクロックを動作基準として動作する。

第３図はディジタル映像圧縮信号のパケットの構成図である。１パケットは固定長、例えば、１８８バイトで構成されており、４バイトのパケットヘッダ３０６と、１８４バイトのパケット情報３０７により構成されている。ディジタル圧縮映像信号は、パケット情報３０７の領域に配置される。また、パケットヘッダ３０７はパケット情報の種類等の情報により構成される。

第４図は第３図のパケットヘッダ３０６の構成図である。５０１はパケットの先頭を示す同期バイト、５０２は誤りの有無を示す誤り表示、５０３はユニットの開始を示すユニット開始表示、５０４はパケットの

重要度を示すパケットプライオリティ、５０５はパケットの種類を示すパケットＩＤ、５０６はスクランブルの有無を示すスクランブル制御、５０７は追加情報の有無及びパケット情報の有無を示すアダプテーションフィールド制御、５０８はパケット単位でカウントアップされる巡回カウンタである。

第５図はディジタル放送の伝送信号及び伝送信号より選択された信号の構成図である。７１は図３のパケットである。通常、上記映像信号に音声信号、プログラムに関する情報等が付加され、複数チャンネルのプログラムが時分割多重されて伝送される。

第５図（ａ）は、３チャンネルのプログラムを多重した例であり、Ｖ１、Ｖ２、Ｖ３はそれぞれのチャンネルの映像信号、Ａ１、Ａ２、Ａ３はそれぞれのチャンネルの音声信号のパケットである。なお、映像または音声は、一つのチャンネルに複数の映像または音声で構成されている場合もある。Ｐ０、Ｐ１、Ｐ２、Ｐ３はプログラムに関する情報である。それぞれのパケットは、異なるパケットＩＤ５０５が割り当てられており、これによりパケットの内容を識別することができる。

Ｐ０は、第５図（ａ）の伝送信号全体に関する情報であり、それぞれのプログラムにどのパケットＩＤが割り当てられているかを認識するためのプログラムアソシエーションテーブル、番組ガイド情報等のパケットが時分割多重されて伝送される。Ｐ１、Ｐ２、Ｐ３は、それぞれのプログラムに関する情報であり、そのチャンネルの映像パケット、音声パケット等にどのパケットＩＤが割り当てられているかを認識するためのプログラムマップテーブル、スクランブル情報等のパケットが時分割多重されて伝送される。通常、プログラムアソシエーションテーブルのパケットＩＤは決まった値、例えば０が割り当てられている。

受信時には、まずプログラムアソシエーションテーブルによって受信

したいプログラムのプログラムマップテーブルにどのパケットＩＤが割り当てられているかを認識し、次に、受信したいプログラムのプログラムマップテーブルによって映像パケット、音声パケット等にどのパケットＩＤが割り当てられているかを認識する。そして、映像パケットおよび音声パケットを抽出してディジタル圧縮データの復号を行う。また、同時にプログラムクロックリファレンスを抽出し、これによってディジタル圧縮データの復号回路の復号タイミングが符号化時のタイミングと同期するように復号回路の動作を制御する。

ＣＲは、ディジタル圧縮データの復号時の同期をとるためのプログラムクロックリファレンス情報である。

もちろん、多重するチャンネル数は３チャンネル以外、例えば４チャンネルでもよいし、また、これ以外の情報を多重してもよい。

第５図（ｂ）は、第５図（ａ）から第１のチャンネルの情報およびそれに関連したプログラム情報のみを選択したものである。第１のチャンネルを記録する場合には、この情報をディジタル放送受信機２０１から記録再生装置２００に出力する。もちろん、これ以外の情報を含めて記録してもよいし、また、再生時の処理をやりやすくするために、パケットの情報の一部を変更してもよい。例えば、プログラムアソシエーションテーブルの情報を記録するプログラムのみの情報に変更すれば、再生時にチャンネルの選択が不要になる。

第６図は第２図のデータ暗号回路１１５の構成図である。１１５１はパケットデータ入力端子、１１５７はパケットデータ出力端子、１１５３ａ、１１５３ｂはデータ鍵入力端子、１１５３ｃはデータ鍵選択信号入力端子、１１５３ｄは、処理モード選択信号入力端子、１１５２、１１５６はブロック処理回路、１１５４は鍵スケジュール回路、１１５５は暗号器、１１５８ａ，１１５８ｂはデータ鍵レジスタ、１１５９はデー

タ鍵セレクタである。データ暗号回路１１５は、あらかじめ定められたデータ鍵により、入力されるパケットデータ単位で暗号化して出力する。この際、このデータ鍵をある時間間隔で変更していくことにより、テープ上に記録されるパケットデータの安全性を高めることができる。

暗号器１１５５は、例えば、伝送中にビット誤り等のエラーが発生しても、そのエラーが後続のデータに影響を与えない、すなわちエラー伝播がないように、複数ビットで構成されるブロックを単位として暗号処理を簡単な回路構成で実現できるブロック暗号を用いる。

入力端子１１５１から入力されたパケットデータは、まず、ブロック処理回路１１５２において、複数ビットからなるブロックＰに区切られる。例えば1ブロックを６４ビットとする。各ブロックは、暗号器１１５５において順次暗号化され、その結果ブロックＣを出力し、ブロック処理回路１１５６において、今度はブロックをパケットデータの形式に戻して出力端子１１５７へ出力する。ここで、暗号化のための鍵であるデータ鍵は、制御回路１０４より、データ鍵入力端子１１５３ａおよび１１５３ｂから入力され、データ鍵レジスタ１１５８ａ、１１５８ｂに記憶される。例えば、データ鍵レジスタ１１５８ａには、現在のデータ鍵を、データ鍵レジスタ１１５８ｂには次に切り換えるデータ鍵を記録させる。

また、データ鍵選択信号入力端子１１５３ｃからは、制御回路１０４より、データ鍵レジスタ１１５８ａ、１１５８ｂのどちらのデータ鍵を選択するかを示す信号が入力され、データ鍵セレクタ１１５９により、選択されたデータ鍵が出力される。ここでは、例えば鍵レジスタ１１５８ａのデータ鍵が選択されているものとする。選択されたデータ鍵は、スケジュール回路１１５４においてサブ鍵ＫＡ、ＫＢに変換され、暗号器１１５５に供給される。例えば、データ鍵の長さ５６ビット、サブ鍵

の長さが、それぞれ３２ビットとし、データ鍵の上位３２ビットをＫＡに割り当て、データ鍵の上位３２ビットと下位３２ビットの加算値をＫＢに割り当てる。

ここで、データ鍵を変更する場合には、制御回路１０４より、データ鍵レジスタ１１５８ｂを出力するようデータ鍵選択信号入力端子１１５３ｃから信号が入力される。データ鍵セレクタは、一つのパケットデータのブロック全ての暗号化が終了するまでは、その選択出力を切り換えず、次のパケットデータとの間で切り換えるよう制御する。

その他、例えば、暗号器１１５５の出力と、暗号器１１５５の入力を排他的論理和をとり、ブロック単位でフィードバックをかけることで、暗号強度を増す方法もある。

第７図は第６図の暗号器１１５５の構成図である。同図中、５５１、５５２、５５３、５５４は暗号処理部、Ｐａ、Ｐｂは入力ブロックデータＰの上位および下位ビット、Ｃａ、Ｃｂは暗号化されたデータ、ＫＡ、ＫＢは、サブ鍵である。同図に示すように、例えば入力された６４ビットのブロックＰを、その上位３２ビットＰａと下位３２ビットＰｂに分離する。そのＰａ、Ｐｂは、暗号処理部５５１において、排他的論理和（５５１１）、ビットシフトおよび加算演算（５５１２、５５１３、５５１５：Ａ＜＜＜ｐは、Ａをｐビット左方向に循環ビットシフトすることを表す）、加算演算（５５１４、５５１６）を行い、その結果を暗号処理部５５１と同様の処理を行う後続の暗号処理部５５２、５５３、さらに図示しない暗号処理部に入力して複数段繰り返し演算を行い、最終段の暗号処理部５５４により出力されたデータＣａ、Ｃｂより、暗号化されたブロックＣを得る。

以上は、第２図、第７図のデータ暗号回路１１５について説明したが、第２図のデータ復号回路１１６では、暗号器１１５５の逆の流れで演算

していくことにより、暗号化されたブロックを復号することができる。ただし、第７図の演算５５１６は、減算処理とする。また、当然、サブ鍵ＫＡ、ＫＢは、暗号時と同一の鍵を用いなければならない。

その他、記録するパケットデータを保護する必要が無い場合、例えば記録する番組が自由にコピーしてもよいよう許可されている場合、パケットデータを暗号化しないで、そのままテープ上に記録する場合がある。これは例えば、データ暗号回路１１５、データ復号回路１１６を、入力パケットの暗号・復号の機能と、なにもしないで通過させる機能とを切り換えることで実現できる。第２図、第６図のデータ暗号回路１１５において、第６図の処理モード選択信号入力端子１１５３ｄを介して入力される処理モード選択信号により、第７図の演算５５１６への入力Ｘ５を、図示していないが、零に固定することで、暗号、復号処理を行わずに、ブロックを通過させることが出来る。この方法によれば、入力パケットの通過遅延時間を一定に保ったまま、動作を切り換えることができる。また、図示しないが、他の方法としては、入力端子１１５１から入力されたパケットデータを、ブロック処理回路１１５２、暗号器１１５５、ブロック処理回路１１５６を介さず、出力端子１１５７に出力するか、ブロック処理回路１１５６から出力されるパケットデータを出力端子１１５７に出力するかを切り換える切り換え回路を出力端子１１５７の前段に設け、処理モード選択信号入力端子１１５３ｄを介して入力される処理モード選択信号をその切り換え回路に入力して、ブロック処理回路１１５６から出力されるパケットデータか、入力端子１１５７に入力されたパケットデータかを切り換える方法もある。これらの方法は、第２図、第１９図のデータ復号回路１１６においても前述と同様の構成で実現できる。

第８図は第２図のデータ暗号回路１１５、データ復号回路１１６に供

給するデータ鍵の生成例を示すところの制御回路１０４内のデータ鍵の生成図である。デバイス鍵発生器１１７は、例えば９６ビットのあらかじめ定められた固定の鍵情報を記憶している。ブロック鍵発生器１１８は、例えば第２図の制御回路１０４からの司令１１８１により、９６ビットの乱数を発生させる乱数発生器である。１２０は９６ビットの排他的論理和演算器、１２１はハッシュ関数演算器である。第8図（ａ）では、ブロック鍵とデバイス鍵は、排他的論理和演算器１２０で排他的論理和がとられ、ハッシュ関数演算器１２１にてハッシュ演算がなされ、その結果のうちの選択された５６ビットが、データ鍵として第2図のデータ暗号回路１１５に供給される。ハッシュ関数は、その出力結果から、入力データが類推困難な関数であり、データ鍵から、秘密情報であるブロック鍵、デバイス鍵が求められない。

また、第2図の制御回路１０４からの司令１１８１をある時間間隔で発生させ、上述の演算によるデータ鍵生成を繰り返し行うことにより、データ鍵を順次変更していくことができ、記録媒体上のデータの安全性を高めることが可能となる。次に、ブロック鍵発生器１１８で発生されたブロック鍵（Ｋｒ）は、第2図の記録信号処理回路１０２ａに送られ、テープ１１１上に記録される。

再生時には、ブロック鍵発生器１１８の発生するブロック鍵の代わりに、テープ１１１上から再生されたブロック鍵（Ｋｐ）を用いて、上記と同様の演算を行い、データ鍵を得、第2図のデータ復号回路１１６に供給される。

第8図（ｂ）は、テープ１１１上に記録する鍵情報Ｋｒとして、ブロック鍵をデバイス鍵で排他的論理和演算したものを用いる例である。この場合、ハッシュ関数演算器にはブロック鍵そのものが入力される。再生時には、第8図（ａ）中のブロック鍵の代わりに、テープ１１１上か

ら再生されたＫｐを用いて、上記と同様の演算を行い、データ鍵を得、データ復号回路１１６に供給される。

次に、テープへの記録方法について述べる。

図９は、１トラックの記録パターンである。３は時間情報、プログラム情報等のサブコードを記録するサブコード記録領域、７はディジタル圧縮映像信号を記録するデータ記録領域、２及び６はそれぞれの記録領域のプリアンブル、４及び８はそれぞれの記録領域のポストアンブル、５はそれぞれの記録領域の間のギャップ、１及び９はトラック端のマージンである。このように、各記録領域にポストアンブル、プリアンブル及びギャップを設けておくことにより、それぞれの領域を独立にアフレコを行うことができる。もちろん、記録領域７にはディジタル圧縮映像信号以外のディジタル信号を記録してもよい。データ記録領域７は、複数のブロック（前述の暗号化の小単位であるブロックとは異なる）により構成されている。

第１０図は第９図のデータ記録領域７のブロックの構成図である。２０は同期信号、２１はＩＤ情報、２２はデータ、２３は第１の誤り検出訂正のためのパリティ（Ｃ１パリティ）である。例えば、同期信号２０は２バイト、ＩＤ情報２１は３バイト、データ２２は９９バイト、パリティ２３は８バイトで構成されており、１ブロックは１１２バイトで構成されている。

第１１図は第１０図のＩＤ情報２１の構成図である。３１はグループ番号、３２はトラックアドレス、３３は１トラック内のブロックアドレス、３５はグループ番号３１、トラックアドレス３２及びブロックアドレス３３の誤りを検出するためのパリティである。ブロックアドレス３３は、各記録領域でのブロックの識別を行うためのアドレスである。例えば、第９図のデータ記録領域７では０～３３５とする。トラックアド

レス３２は、トラックの識別を行うためのアドレスであり、例えば、１トラックまたは２トラック単位でアドレスを変化させ、ｎトラックを識別することが出来る。例えば、０～５または０～２とすることにより、６トラックを識別することができる。第１１図のグループ番号３１は、例えば、トラックアドレス３２で識別する６トラック単位で変化させ、０～１５とすることにより、９６トラックを識別することができる。トラックアドレス３２は、後述する第２の誤り訂正符号の周期と同期させておけば、記録時の処理及び再生時の識別を容易にすることができる。

第１２図は第９図のデータ記録領域７の１トラック分のデータの構成図である。なお、第１０図に図示の同期信号２０およびＩＤ情報２１は省略してある。データ記録領域７は、例えば、３３６ブロックで構成されており、最初の３０６ブロックにデータ４１を、次の３０ブロックに第２の誤り訂正符号（Ｃ２パリティ）４３を記録する。Ｃ２パリティ４３は、ｎトラック単位、例えば６トラック単位で構成されている。６トラック単位でみると、データは３０６ブロック×６トラックのデータであり、そのデータを１８分割して、それぞれの１０２ブロックに、１０ブロックのＣ２パリティを付加する。誤り訂正符号は、例えばリードソロモン符号を用いればよい。各ブロック９９バイトのデータは、３バイトのヘッダ４４と９６バイトのデータ４１により構成されている。

第１３図は、１８８バイトのパケット形式で伝送されたディジタル圧縮映像信号を、第１２図のデータ４１に記録する時の１パケットのブロックの構成例である。この場合には、４バイトの時間情報２５を付加して１９２バイトとし、２ブロックに１パケットを記録する。時間情報２５は、パケットの伝送された時間の情報である。すなわち、パケットの先頭が伝送された時の時間またはパケット間の間隔を基準クロックでカウントし、そのカウント値をパケットデータと共に記録しておき、再生

時にその情報を基にしてパケット間の間隔を設定することにより、伝送された時と同一の形でデータを出力することができる。

第１４図は第１２図のデータ記録領域７のヘッダ４４の構成図である。ヘッダ４４は、フォーマット情報４５、ブロック情報４６および付加情報４７により構成される。フォーマット情報４５、およびブロック情報４６には、記録に関する様々な記録情報が、また付加情報４７には、その他補助的な情報が記録される。

フォーマット情報４５は、記録フォーマットに関する情報であり、記録モード（標準速モードその他の識別）、取り扱うパケットデータの種類、記録されているパケットデータがコピー可能か否か等を示すコピー制限情報等が格納され、複数のブロックで、１つの情報を構成する。例えば１２ブロックの１２バイトで１つの情報を構成している。そして、この情報を複数回繰り返し多重記録することにより、再生時の検出能力を向上させている。ここに、前述の鍵情報等をも記録しておくことが可能である。

ブロック情報４６は、データ記録領域４１に記録されるデータの種類を識別するための情報である。ここには、高速可変速再生用データの有無、種類（どの速度に対応した高速可変速再生用データであるか）等を記録しておく。ここに、前述の鍵情報等をも記録しておくことも可能である。

付加情報４７は、例えば、６ブロックの６バイトで一つの情報であるパックデータを構成し、最初の１バイトが情報の種類を表すアイテムコード、残りの５バイトをデータとすることにより、いろいろな種類のデータを記録することができる。例えばここに前述のブロック鍵等の鍵情報や、その他、記録時間等の情報や記録信号の種類等を記録しておくことができる。

第１５図は第１４図の付加情報４７の領域に、ブロック鍵を格納する場合のパックデータの構成図である。

パックデータの最初の１バイトには後続の情報が鍵情報であることを示すアイテム情報コードを格納する。

２バイト目には、格納されている鍵の種類を示す情報（鍵シーケンス番号、鍵属性、鍵フラグ）を記録する。前述のように、ブロック鍵をある時間間隔で順次変更していくことで、記録媒体上のデータの安全性を高めることができるので、例えば、このパックに格納されているブロック鍵が、現在のパケットデータの暗号化に用いられるブロック鍵か、次に用いるブロック鍵かを示す鍵属性情報を記録しておく。また、ブロック鍵が更新される度に反転する鍵フラグで、切り換えタイミングを記録する。この情報により再生時の鍵の切り換えをスムーズにする。また、鍵シーケンス番号には、一つのパックでブロック鍵が格納できない場合、後続のパックがあることを示す情報を格納する。例えばブロック鍵が９６ビットの場合、３つのパックに分割して格納し、それぞれの鍵シーケンス番号には、２、１、０を格納し、０が最終パックであることを示す。その他、全体のデータのサイズを格納しておき、残りの大きさを知る方法もある。

３バイト目から６バイト目に、ブロック鍵を収納する。

前述の第８図（ｂ）の例では、鍵情報Ｋｒがブロック鍵の代わりに格納される。

第１６図はブロック鍵の格納方法を示す図である。この例は、各トラックのパックデータには、現在の鍵情報のみを記録する場合である。したがって、前述の鍵属性は、現在の鍵を示すのみの固定情報であり、記録しなくてもよい。同図中（１）は、９６ビットの現在のブロック鍵Ａ（Ａ０乃至Ａ１１）が３個のパックに分割して格納される状態を示す。

通常、これらのパックは、データの信頼性の向上のため、一つのトラックにつき、複数回記録される。例えば、3個のパックをトラックの最初、半ば、最後のそれぞれの領域に記録する（計9個）ことで、磁気ヘッドの目詰まり等による、再生信号のバースト欠落の影響を軽減できる。また、3個のパックは必ずしも連続したパックとして記録する必要はなく、各パックの間に他の情報を格納したパックを挿入し、鍵情報を格納しているパックを分散して記録することで、鍵情報自身の保護も可能となり、さらに信頼性が向上する。同図（2）はブロック鍵がBに切り換わったトラックに記録されるパックデータである。この場合、ブロック鍵Bの鍵フラグは反転している。

第17図はブロック鍵の他の格納方法を示す図である。第17図は、現在の鍵情報と共に、次に使用する鍵情報もあらかじめ発生させておき記録する方法である。ここで、鍵属性情報は、現在のパケットデータの暗号化に用いられるブロック鍵の場合“0”、次に用いるブロック鍵の場合“1”とする。また、ブロック鍵が更新される度に反転する鍵フラグは“0”と“1”を交互に繰り返す。

同図中（1）は、96ビットの現在のブロック鍵Aが格納される状態を示す。（2）には、次のブロック鍵Bが格納される。この（1）および（2）が、同一のトラック内のブロックの付加情報エリアに記録される。（3）は、ブロック鍵がBに切り換わったトラックに記録されるパックデータである。この場合、ブロック鍵Bは、鍵属性情報“0”の現在の鍵に、また、鍵フラグも反転している。さらに（4）は、次に用いる鍵Cが格納される。（3）および（4）が、同一のトラック内のパックデータとしてトラックに記録される。

ブロック鍵の更新タイミングを示す鍵フラグの格納場所としては、付加情報47のパックに格納する以外に、前述の第14図に示したフォー

マット情報４５、あるいはブロック情報４６に格納する方法もある。

以上のように、鍵情報が、テープ上に記録されるが、ブロック鍵を切り換えるタイミングとしては、前述のＣ２パリティの付加の単位であるｎトラック（本実施例では６トラック）の区切り目とすることで、再生時に、Ｃ２パリティの演算が可能となり、鍵情報のデータ信頼性が向上する。

また、以上の例ではブロック鍵が更新されるタイミングを示す情報を鍵フラグとして記録したが、第２図の記録信号処理回路１０２aにおいて、前述の第１１図に示したトラックアドレス３２、あるいはグループ番号３１の値と、Ｃ２パリティの演算の周期および更新のタイミングを同期させることで、特に鍵フラグを記録しなくとも、再生時における鍵情報の更新のタイミングを、このトラックアドレス３２あるいはグループ番号３１の値で検出することも可能である。例えば、第２図の記録信号処理回路１０２aにおいて、トラックアドレス３２が、トラック１本毎に０から５の値を繰り返し、その値０から５の６本のトラックを、前述のＣ２パリティの付加の単位とする。そして、値が５から０になるタイミングで、データ暗号回路１１５において、ブロック鍵を更新して、記録する。再生時においては、第２図の再生信号処理回路１０２bにおいて、このトラックアドレス３２の値が５から０になるタイミングを検出し、データ復号回路１１６において、鍵を更新していけばよい。また、さらに長い周期で更新する場合には、例えば、グループ番号３１を用いて、トラックアドレス３２の値が５から０になる際に、グループ番号３１を１増加させ、０から１５の値を繰り返すようにすることで、９６トラックの単位で、しかもＣ２パリティの付加の単位の区切り目の、更新のタイミングを検出することが可能となる。

第１８図は第１３図の時間情報２５（４バイト＝３２ビット）の具体

20

的構成例であり、鍵フラグ、暗号フラグ格納の他の方法を示したものである。ここでは、例えば、時間情報２５１としては、２２ビットの情報であり、２５２は前述の鍵フラグ（１ビット）、２５３は、後続のパケットデータが暗号化されているかどうかを示す暗号フラグ（１ビット）である。記録時には、第２図の入出力制御回路１１９は、タイムスタンプである時間情報２５１とともに、暗号フラグ２５３に、後続のパケットデータが暗号化されている場合には例えば“１”を、暗号化されていない場合には“０”を格納し、また、鍵フラグ２５２には、後続のパケットデータに対応する前述の鍵情報を格納するパックデータの鍵フラグを格納する。再生時には、第２図の入出力制御回路１１９において、記録時に付加した時間情報２５を取り除いてデータ復号回路１１６に出力するとともに、暗号フラグ２５３、鍵フラグ２５２をデータ復号回路１１６に供給し、データ復号回路１１６の動作を制御する。

第１９図は第２図のデータ復号回路１１６の構成図である。１１６１はパケットデータ入力端子、１１６７はパケットデータ出力端子、１１６３ａ、１１６３ｂはデータ鍵入力端子、１１６３ｃはデータ鍵選択信号入力端子、１１６３ｄは、処理モード選択信号入力端子、１１６２、１１６６はブロック処理回路、１１６４は鍵スケジュール回路、１１６５は復号器、１１６８ａ，１１６８ｂはデータ鍵レジスタ、１１６９はデータ鍵セレクタである。データ復号回路１１６は、あらかじめ定められたデータ鍵により、入力されるパケットデータ単位で復号化して出力する。

復号器１１６５は、複数ビットで構成されるブロックを単位として復号処理を実現するブロック暗号を用いる。

入力端子１１６１から入力されたパケットデータは、データ暗号回路１１５と同様に、複数ビットからなるブロックＣに区切られ、各ブロッ

クは、復号器１１６５において順次復号化され、その結果ブロックＰを出力し、ブロック処理回路１１６６において、パケットデータの形式に戻して出力端子１１６７へ出力する。ここで、復号化のための鍵であるデータ鍵は、制御回路１０４より、データ鍵入力端子１１６３ａおよび１１６３ｂから入力され、データ鍵レジスタ１１６８ａ、１１６８ｂに記憶される。例えば、データ鍵レジスタ１１６８ａには、現在のデータ鍵を、データ鍵レジスタ１１６８ｂには次に切り換えるデータ鍵を記録させる。

また、処理モード選択信号入力端子１１６３ｄからは、入出力制御回路１０９より検出した暗号フラグ２５３が入力され、復号器１１６５を復号動作のモードか、何もしないで通過させるモードかを決定する。さらに、データ鍵選択信号入力端子１１６３ｃからは、入出力制御回路１０９より検出した鍵フラグ２５２が入力され、データ鍵セレクタ１１６９により、選択されたデータ鍵が出力される。選択されたデータ鍵は、スケジュール回路１１６４においてサブ鍵ＫＡ、ＫＢに変換され、暗号器１１６５に供給される。

ここで、第２図の入出力制御回路１１９で検出した、暗号フラグ、あるいは鍵フラグが変化すると、それに連動して、データ復号器１１６の動作モード、データ鍵の選択が行われる。

以上のように、各パケットデータへ暗号フラグ、鍵フラグを付加することにより、パケットデータ単位での、暗号化の有無、鍵情報の判別、および復号処理が実現できる。

その他、暗号化されているかどうかを示す暗号フラグの格納場所としては、第１５図に示した鍵情報を格納するパックの2バイト目に格納する方法、あるいは前述の第１４図に示したフォーマット情報４５、ブロック情報４６に格納する方法もある。

暗号フラグをフォーマット情報４５、あるいはブロック情報４６等に格納することで、例えば暗号フラグが“１”を示す時、すなわちパケットデータが暗号化されている場合には、データ復号回路１１６の動作を復号動作とするとともに、付加情報４７の鍵情報を格納するパックから、鍵情報を取得するようにし、暗号フラグが“０”の場合は、データ復号回路１１６の動作を、復号しないでそのまま出力するようにすることで、パケットデータが暗号化されていない場合の制御動作の簡略化が図れる。また、暗号フラグを鍵情報を格納するパックに格納する方法では、暗号フラグが“０”、すなわちパケットデータが暗号化されていない場合は、そのパックの３バイト目以降のブロック鍵情報は格納されていない。

その他、暗号フラグを用いずに、例えば、鍵情報を格納するパックの有無で暗号化されているかどうかを判別することもできる。

第２０図は第２図の記録信号処理回路１０２ａおよび再生信号処理回路１０２ｂからなるディジタル記録再生信号処理回路１０２の構成図である。４００はメモリ回路、４０１は第２図の制御回路１０４に従いメモリ回路４００を制御するアドレス等を生成するメモリ制御回路、４０２はＣ２パリティ演算回路、４０３はＣ１パリティ演算回路、４０４は前記制御回路１０４からの設定内容に従い記録時のＩＤ情報、サブコード生成、フォーマット情報、ブロック情報、鍵情報等の付加情報の付加、および再生時のＩＤ情報、サブコード、フォーマット情報、ブロック情報、鍵情報等の付加情報の取得等を行う付加情報処理回路、４０５は記録時の変調処理及び再生時の復調処理を行う変復調回路である。本実施例では、一例としてＣ２パリティ演算を行うために６トラックのデータを必要とするため、メモリ回路４００は少なくとも６トラック分のデータを蓄積する容量を備えるものとする。

記録時には、端子４１１、４１３を介して第２図の制御回路１０４に

より、記録状態に設定される。第２図のデータ暗号回路１１５で暗号化されたパケットデータが端子４１０から入力され、メモリ制御回路４０１の制御信号に従いメモリ回路４００に蓄積される。Ｃ２パリティ演算に必要なデータが蓄積された後、メモリ回路４００から逐次読みだされ、Ｃ２パリティ演算回路４０２に入力されて、所定の演算が行われる。Ｃ２パリティ演算回路４０２で得られた演算結果は、メモリ回路４００に蓄積される。一方、端子４１３を介して第２図の制御回路１０４からの設定に従い、付加情報処理回路４０４で、入力された暗号化パケットデータの鍵に対応した鍵情報等のパックデータが生成され、メモリ回路４００に蓄積される。さらに前記した記録ブロックを構成するように、鍵情報等を含めメモリ回路４００から読みだされたデータは、Ｃ１パリティ演算回路４０３でＣ１パリティを付加され、変復調回路４０５に入力される。変復調回路４０５で所定の変調処理された信号は、端子４１４を介して出力され、第２図の記録再生アンプ１１６、回転ヘッド１００を介してテープ１１１上に記録される。

第２１図はデータ記録開始時における信号処理のタイミングを示す図である。第２１図（ａ）はデータ暗号化回路１１５から入力されるパケットデータ、第２１図（ｂ）は、データ暗号化回路１１５が暗号化の際に用いたデータ鍵、第２１図（ｃ）は、前述のＣ２パリテイ４３の６トラック単位構成にあわせて、第２０図のＣ２パリティ演算回路４０２でのＣ２パリティ演算サイクル（本実施例では６トラック）を示し、第２１図（ｄ）は回転ヘッド１００を介してテープ１１１に記録する記録信号を示している。第２１図の実施例では、記録開始が設定される時間ｔ１より前にあらかじめブロック鍵Ａを生成し、データ鍵Ｋａを演算して、データ暗号化回路１１５に供給しておく。また、記録開始が設定される時間ｔ１より前は、記録信号処理回路１０２ａは入力信号に関らずパケ

ット無しとみなして記録信号処理を行うように制御する。これにより、時間ｔ０に記録開始が設定されても、期間ｐ０のデータに対してのＣ２パリティの演算は可能となる。

第２図の制御回路１０４は、時間ｔ０で記録開始にした時の入力データのＣ２パリティ演算サイクルｓ０が終了して、前記第２の誤り訂正符号を構成するｎトラック（本実施例では６トラック）の先頭から記録信号を出力する（第２１図（ｄ））ように制御する。また、データ鍵は、このＣ２パリティの演算サイクルで更新される。例えば、時間ｔ２より前にブロック鍵Ｂを生成し、データ鍵Ｋｂを演算してデータ暗号化回路１１５に供給しておき、時間ｔ２の時点でデータ暗号化回路１１５においてデータ鍵をＫｂに切り換える。通常、データ暗号化回路１１５は、その処理のため、パケットデータの入力から出力までの間に遅延時間が生じる。そこで、時間ｔ２からデータ暗号化回路１１５がパケットを暗号化処理することにより生じるデータ遅延時間分前の時点で、データ暗号化回路１１５に供給するデータ鍵をＫｂに切り換える。あるいは、データ鍵が切り換えられたパケットデータからは、次の演算サイクルの処理に先送りしてもよい。この実施例では、先頭部分に余分なデータが記録されるが、記録開始にする時間ｔ１のタイミングによらず、記録すべき信号に対しＣ２パリティを付加し、上記Ｃ２パリティ演算サイクル単位で記録できる。また、再生時において、先頭の余分なデータ部分は、パケット無しとみなして記録処理しているので、Ｃ２パリティ演算に用いられるだけで、出力されることはない。

記録終了時には、前記記録再生信号処理回路１０２ａの、テープ１１１への記録動作を、複数トラックのデータを用いて演算するＣ２パリティの演算サイクル（本実施例では６トラック）完結で行うように前記制御回路１０４で制御する。この制御方式により、記録開始、記録終了の

切換えタイミングによらず、テープ１１１上の記録データに全てＣ２パリティを付加し、Ｃ２パリティの演算サイクル単位で鍵情報が更新されパケットデータが暗号化されるので、再生時には、Ｃ２パリティ演算サイクル単位で再生でき、Ｃ２パリティ演算が可能となるので、鍵情報のデータ信頼性も向上する。

第２２図は第２図のテープ１１１上の鍵情報を示す図である。同図中、１１１１から１１１７は、Ｃ２パリティ演算サイクルである６トラック単位で示した記録トラックである。この図の場合、記録トラック１１１１から１１１３までが、ブロック鍵Ａ、記録トラック１１１４から１１１６までがブロック鍵Ｂをもとに暗号化されたパケットデータ、およびそれらに対応した鍵情報であるパックデータが格納される。また、記録トラック１１１７は暗号化されずに記録されたトラックである。この図のように、暗号化されたトラックと、暗号化されていないトラックが同一のテープ上に混在することも可能である。鍵情報の更新は、例えば、４８トラック、９６トラック等、ｍ×ｎトラック毎（ｍは１以上の整数、ｎは本実施例では６）、あるいは一つの番組全体等考えられるが、鍵の切り換わり目、あるいは暗号化されたトラックと、暗号化されていないトラックとの境目は、Ｃ２パリティ演算サイクル（本実施例では６トラック）の区切り目である。

以上、記録の際の動作について説明した。ここで、鍵情報をサブコード領域（第９図の７）に記録することも可能であるが、鍵情報を、各ブロックのヘッダ（第１２図の４４）の部分に格納し、各トラック上のデータ記憶領域（第９図の７）に記録することで、アフレコ等による鍵情報のみの書き換えは困難となる。従って、鍵情報の消失を防ぐことができ、また、故意に鍵情報のみを改ざんして意図的に暗号通信を行うことはできない効果がある。

次に、テープからの再生方法について述べる。

第２０図のディジタル記録再生信号処理回路１０２において、再生時は、端子４１１、４１３を介して第２図の制御回路１０４によって、再生状態に設定される。前記テープ１１１から回転ヘッド１００で再生され、端子４１４から入力された再生信号は、変復調回路４０５で復調処理された後、Ｃ１パリティ演算回路４０３でＣ１パリティ演算を行い、誤り検出およびその訂正を行い、Ｃ１パリティ演算結果も一緒にメモリ回路４００に蓄積される。Ｃ２パリティ演算に必要なデータが蓄積された後、メモリ制御回路４０１の制御信号に従いメモリ回路４００から逐次読みだされ、Ｃ２パリティ演算回路４０２に入力される。Ｃ２パリティ演算回路４０２では、上記データで演算を行い、誤りの検出、訂正処理したデータおよびＣ２パリティ演算結果を、再びメモリ回路４００に蓄積する。

第２図のタイミング生成回路１０５から端子４１２を介して入力されるタイミング信号を基準として所定の順番にメモリ回路４００からデータを読みだし、前記Ｃ１パリティ、Ｃ２パリティの演算結果を参照し、誤りの無いデータのみを端子４１０から第２図の入出力制御回路１１９に出力する。一方、付加情報処理回路４０４では、メモリ回路４００から読み出したデータから鍵情報やサブコード等を取得し、端子４１３を介して第２図の制御回路１０４に送出する。その後、第８図で示した演算、すなわち再生によって得られた鍵情報から、Ｋｐを取り出し、デバイス鍵発生器１１７からのデバイス鍵との排他的論理和をとって、ハッシュ関数１２１の演算を行い、データ鍵を得、第２図のデータ復号回路１１６に出力する。このデータ鍵は、記録時に用いたデータ鍵と同一のものであり、データ復号回路１１６において、正しくもとのパケットデータを得ることができる。

第２３図は、本発明のデータ再生時における信号処理のタイミングを示す図である。第２３図（ａ）は回転ヘッド１００を介してテープ１１１から再生される再生信号、第2.3図（ｂ）は上記Ｃ２パリティの演算サイクル（本実施例では６トラック）を示し、第２３図（ｃ）は入出力制御回路１１９から出力されるパケットデータを示し、第２３図（ｄ）は、第２図のデータ復号回路１１６に供給されるデータ鍵を示している。付加情報処理回路４０４では、演算サイクルｓ３においては、このサイクルで用いられている鍵情報ＫｐＣが検出されている。このＫｐＣにより前述の演算で得られたデータ鍵Ｋｃが、例えば前述のデータ鍵レジスタ１１６３ａに記憶されており、データ鍵セレクタ１１６９も、データ鍵レジスタ１１６３ａのデータ鍵Ｋｃが出力されるように選択されている。

次に、演算サイクルｓ４において、鍵情報ＫｐＤが用いられていることが検出されると、あらかじめ、データ鍵Ｋｄを前述の演算で求めておき、データ鍵レジスタ１１６３ｂに記憶させ、時間ｔ３のタイミングで、データ鍵セレクタ１１６９を制御してデータ鍵レジスタ１１６３ｂのデータ鍵Ｋｄに切り換える。以上の方法により、データ鍵を更新しながらの再生動作が可能となる。

また、既に記録済みのテープに追加記録する場合、Ｃ２パリティの付加単位の区切り目から、記録を開始するようにすることで、追加記録直前のトラックの鍵情報のデータ信頼性を損なわずに、つなぎ記録が可能となる。

その他、パケットデータが暗号化されているかいないかを区別する方法としては、第４図で示した同期バイト５０１は、通常固定データであるので、例えば、再生信号処理回路１０２ｂにおいて、この同期バイトの検出を行い、検出できた場合は、第２図のデータ復号回路１１６を入

力されるパケットデータを何もしないで通過させる機能に切り換え、検出できなかった場合は、第２図のデータ復号回路１１６を復号機能の動作に切り換え、付加情報エリア内の鍵情報を検出する動作を行うことで、記録時に、パケットデータを暗号化して記録されたトラックと、暗号化しないで記録したトラックとが混在するテープの場合にも、検出が可能となる。

また、あらかじめ記録されているソフトテープについても、以上説明した方法で、ソフトテープの作成および再生が可能となり、テープ上のパケットデータの保護が実現できる。

以上は、記録トラックに現在のブロック鍵が格納されている例を示したが、データ鍵の演算は、Ｃ２の一演算サイクル内で行わなければならない。Ｃ２の一演算サイクル内でデータ鍵の演算が間に合わない場合は、前述のように、記録トラック内に、現在のブロック鍵と、次のブロック鍵を記録しておくことで、あらかじめ、次のデータ鍵を求めておける。

第２４図は第１図のディジタル信号記録再生装置２００の他の構成図である。同図中、１２１は、例えばＩＥＥＥ１３９４のような高速ディジタルバスインターフェース等のプロトコルを実現するディジタルインターフェース回路であり、入力されたパケットデータの時間間隔を維持しながら、高速にデータを伝送する機能を有する、１２２は、ディジタルインターフェースバスである。１２３は、ディジタルインターフェース１２２上を伝送されるディジタルデータを保護するための暗号／復号回路であり、パケットデータを暗号化してディジタルインターフェースバス１２２上に伝送し、あるいは受信したディジタルデータを復号化する。１２４は、マイクロプロセッサのような制御回路であり、ディジタルインターフェース回路１２１、暗号／復号回路１２３を制御する。

記録時には、ディジタルインターフェースバス１２２上を伝送されて

きた暗号化されたディジタルデータをディジタルインターフェース回路１２１において、所定のパケット処理を行い、暗号／復号回路１２３において、元のパケットデータに復号して、入出力回路１０７に出力する。その後、前述で説明したように、データ暗号回路１１５でパケットデータを暗号化し、テープ１１１上に記録する。再生時には、データ復号回路１１６において、再生したパケットデータを復号化して、入出力回路１０７から暗号／復号回路１２３に出力し、暗号／復号回路１２３において暗号化して、ディジタルインターフェース回路１２１から、ディジタルインターフェースバス１２２に出力する。これによれば、テープ上のパケットデータ、ディジタルインターフェースバス上のパケットデータの双方の保護が実現できる。

なお、以上の実施例では、テープでの記録再生について説明したが、光ディスクや磁気ディスクなどのディスクや、半導体メモリ等、他のあらゆる記録媒体に記録再生する場合でも、同様に適用することができる。

上記ディスクの場合には、鍵情報の切り換え、あるいは暗号化するかしないかの切り換えは、例えばディスクの記録の一つの単位であるセクタの区切り目で行うとよい。

また、上記半導体メモリの場合には、鍵情報の切り換え、あるいは暗号化するかしないかの切り換えは、例えば半導体メモリの記録の一つの単位であるアドレスの区切り目で行うとよい。

また、本実施例は、本発明を、ディジタル信号を鍵により暗号化するシステムに適用したものである。しかし、本発明はこの実施例に限定されるものではなく、例えば、ディジタル信号がキーコードによりスクランブルされたりするシステムにも適用可能である。すなわち、本発明は、少なくとも、ディジタル信号が元々のクリアな状態から変換されるように処理されるあらゆるシステムに対して適用可能なものである。

産業上の利用可能性

本発明によれば、ディジタル信号を、記録媒体上に記録または再生するディジタル信号記録装置、再生装置、および記録媒体において、記録時には、鍵情報に所定の演算を施して得られた鍵で、ディジタル信号を暗号化して、前記鍵情報とともに、記録媒体に記録し、再生時には、記録媒体から再生した前記鍵情報に、前記所定の演算を施して得られた鍵で、再生したディジタル信号を復号化して出力する。以上により、再生の際には、前記所定の演算を施さない限り、前記鍵が得られないので、記録媒体上の鍵情報を得ても、それを用いて暗号化されたディジタル信号を復号することは困難であり、記録媒体上のディジタル信号の著作権を保護することができる。

請求の範囲

1．ディジタル信号を記録媒体上に記録するディジタル信号記録装置において、

少なくとも一つの鍵情報を発生する鍵情報発生手段と、

前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、

前記鍵と前記ディジタル信号が入力され、前記鍵で前記ディジタル信号を暗号化して出力する暗号変換手段と、

少なくとも一つの前記鍵情報を、暗号化された前記ディジタル信号と共に、前記記録媒体上の所定の領域に記録する記録手段とを

備えたことを特徴とするディジタル信号記録装置。

2．前記ディジタル信号は、所定長のパケット形式を有してなることを特徴とする請求の範囲第1項記載のディジタル信号記録装置。

3．前記鍵情報発生手段は、所定時間間隔で少なくとも一つの前記鍵情報を更新していく機能を備え、

前記記録手段は、前記鍵情報発生手段が前記鍵情報を更新するタイミングを識別可能な情報を、前記記録媒体上の所定の領域に記録する機能を備えたことを特徴とする請求の範囲第1項記載のディジタル信号記録装置。

4．前記ディジタル信号は、所定長のパケット形式を有してなり、

前記記録手段は、前記鍵情報発生手段が前記鍵情報を更新するタイミングを識別可能な情報を、前記ディジタル信号の各パケットに付加して前記記録媒体上に記録する機能を備えたことを特徴とする請求の範囲第3項記載のディジタル信号記録装置。

5．前記暗号変換手段は、さらに、前記ディジタル信号を暗号化して出

力する機能と、暗号化しないでそのまま出力する機能とを選択できる機能を備え、

前記記録手段は、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を前記記録媒体上の所定の領域に記録し、暗号化しない場合は、前記鍵情報を記録しない機能を備えたことを特徴とする請求の範囲第1項記載のディジタル信号記録装置。

6．前記ディジタル信号は、所定長のパケット形式を有してなり、

前記記録手段は、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を、前記ディジタル信号の各パケットに付加して前記記録媒体上に記録する機能を備えたことを特徴とする請求の範囲第5項記載のディジタル信号記録装置。

7．所定長のパケット形式のディジタル信号を入力して、別の所定長に分割し、同期信号、記録情報信号、付加情報信号、および第1の誤り訂正符号を付加してブロック形式とし、所定数個のブロックを1トラックとし、n（nは1以上の整数）トラック単位で第2の誤り訂正符号を付加し、前記第2の誤り訂正符号も分割して第1の誤り訂正符号を付加してブロック形式とし、記録媒体上に前記トラックを記録するディジタル信号記録装置において、

少なくとも一つの鍵情報を発生する鍵情報発生手段と、

前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、

前記鍵と前記ディジタル信号が入力され、前記鍵で前記ディジタル信号を暗号化して出力する暗号変換手段と、

少なくとも一つの前記鍵情報を、暗号化された前記ディジタル信号と共に、前記記録媒体上の所定の領域に記録する記録手段とを

備えたことを特徴とするディジタル信号記録装置。

8．前記記録手段は、前記鍵情報を、前記ブロックの付加情報信号領域に格納して前記記録媒体上に記録する機能を備えたことを特徴とする請求の範囲第7項記載のディジタル信号記録装置。

9．前記鍵情報発生手段は、所定時間間隔で少なくとも一つの前記鍵情報を更新していく機能を有し、

前記記録手段は、前記鍵情報発生手段が前記鍵情報を更新するタイミングを識別可能な情報を前記記録媒体上の所定の領域に記録することを特徴とする請求の範囲第7項記載のディジタル信号記録装置。

10．前記記録手段は、前記タイミングを識別可能な情報を、前記ブロックの記録情報信号領域に格納して前記記録媒体上に記録する機能を備えたことを特徴とする請求の範囲第9項記載のディジタル信号記録装置。

11．前記記録手段は、前記タイミングを識別可能な情報を、前記ブロックの付加情報信号領域に格納して前記記録媒体上に記録する機能を備えたことを特徴とする請求の範囲第9項記載のディジタル信号記録装置。

12．前記記録手段は、前記タイミングを識別可能な情報を、前記ディジタル信号の各パケットに付加して前記記録媒体上に記録する機能を備えたことを特徴とする請求の範囲第9項記載のディジタル信号記録装置。

13．前記鍵情報発生手段は、前記第2の誤り訂正符号を付加したnトラックの単位の区切り目で、前記鍵情報を更新していく機能を備えたことを特徴とする請求の範囲第9項記載のディジタル信号記録装置。

14．前記暗号変換手段は、前記ディジタル信号を暗号化して出力する機能と、暗号化しないでそのまま出力する機能とを選択できる機能を有し、

前記記録手段は、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を前記記録媒体上の所定の領域に記録し、暗号化しない場合は、前記鍵情報を記録しない機能を備えたことを特徴とする請求の

範囲第７項記載のディジタル信号記録装置。

１５．前記記録手段は、前記暗号フラグ情報を、前記ブロックの記録情報信号領域に格納して前記記録媒体上にする機能を備えたことを特徴とする請求の範囲第１４項記載のディジタル信号記録装置。

１６．前記記録手段は、前記暗号フラグ情報を、前記ブロックの付加情報信号領域に格納して前記記録媒体上にする機能を備えたことを特徴とする請求の範囲第１４項記載のディジタル信号記録装置。

１７．前記記録手段は、前記暗号フラグ情報を、前記ディジタル信号の各パケットに付加する機能を備えたことを特徴とする請求の範囲第１４項記載のディジタル信号記録装置。

１８．前記暗号変換手段は、前記第２の誤り訂正符号を付加したｎトラックの単位の区切り目で、前記ディジタル信号を暗号化するか否かを切り換える機能を備えたことを特徴とする請求の範囲第１４項記載のディジタル信号記録装置。

１９．記録媒体上に記録されているディジタル信号を再生するディジタル信号再生装置において、

前記記録媒体上の所定の領域に記録されている少なくとも一つの鍵情報と、前記ディジタル信号とを再生する再生手段と、

前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、

前記鍵と再生された前記ディジタル信号が入力され、前記鍵で前記ディジタル信号を復号化して出力する復号変換手段とを

備えたことを特徴とするディジタル信号再生装置。

２０．前記ディジタル信号は、所定長のパケット形式を有してなることを特徴とする請求の範囲第１９項記載のディジタル信号再生装置。

２１．少なくとも一つの他の鍵情報を発生する、鍵情報発生手段を備え、

前記鍵発生手段は、前記鍵情報と、前記他の鍵情報とが入力されて所定の演算を行って鍵を発生する機能を備えたことを特徴とする請求の範囲第１９項記載のディジタル信号再生装置。

２２．前記再生手段は、前記記録媒体上の所定の領域に記録されているところの、更新された前記鍵情報と、前記鍵情報を更新するタイミングを識別可能な情報とを、再生する機能を備え、

前記鍵発生手段は、少なくとも前記更新された鍵情報が入力され、所定の演算を行って更新された鍵を発生する機能を備え、

前記復号変換手段は、入力された前記鍵を、前記タイミング信号に合わせて前記更新された鍵に切り換える手段を備えたことを特徴とする請求の範囲第１９項記載のディジタル信号再生装置。

２３．前記ディジタル信号は、所定長のパケット形式を有してなり、

前記再生手段は、前記ディジタル信号の各パケットに付加して記録されているところの、前記タイミングを識別可能な情報を、再生する機能を備えたことを特徴とする請求の範囲第２２項記載のディジタル信号再生装置。

２４．前記再生手段は、前記記録媒体上の所定の領域に記録されているところの、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を、再生する機能を備え、

前記復号変換手段は、前記暗号フラグ情報により、再生された前記ディジタル信号を復号化して出力する機能と、復号化しないでそのまま出力する機能とを選択して切り換える機能を備えたことを特徴とする請求の範囲第１９項記載のディジタル信号再生装置。

２５．前記ディジタル信号は、所定長のパケット形式を有してなり、

前記再生手段は、前記ディジタル信号の各パケットに付加されて記録されているところの、前記ディジタル信号が暗号化されているか否か示

す暗号フラグ情報を、再生する機能を備えたことを特徴とする請求の範囲第２４項記載のディジタル信号再生装置。

２６．所定長のパケット形式のディジタル信号を別の所定長に分割し、同期信号、記録情報信号、付加情報信号、および第１の誤り訂正符号を付加してブロック形式とし、所定数個のブロックを１トラックとし、ｎ（ｎは１以上の整数）トラック単位で第２の誤り訂正符号を付加し、前記第２の誤り訂正符号も分割して第１の誤り訂正符号を付加してブロック形式とし、記録媒体上に記録されている前記ディジタル信号を再生するディジタル信号再生装置において、

前記記録媒体上の所定の領域に記録されている少なくとも一つの鍵情報と、前記ディジタル信号とを再生する再生手段と、

前記鍵情報が入力され、所定の演算を行って鍵を発生する鍵発生手段と、

前記鍵と再生された前記ディジタル信号が入力され、前記鍵で前記ディジタル信号を復号化して出力する復号変換手段とを

備えたことを特徴とするディジタル信号再生装置。

２７．少なくとも一つの他の鍵情報を発生する、鍵情報発生手段を備え、

前記鍵発生手段は、前記鍵情報と、前記他の鍵情報とが入力され、所定の演算を行って鍵を発生する機能を備えたことを特徴とする請求の範囲第２６項記載のディジタル信号再生装置。

２８．前記再生手段は、前記記録媒体上の前記ブロックの付加情報信号領域に記録されているところの、前記鍵情報を、再生する機能を備えたことを特徴とする請求の範囲第２６項記載のディジタル信号再生装置。

２９．前記再生手段は、前記記録媒体上の所定の領域に記録されているところの、更新された前記鍵情報と、前記鍵情報を更新するタイミングを識別可能な情報とを、再生する機能を備え、

前記鍵発生手段は、少なくとも前記更新された鍵情報が入力され、所定の演算を行って更新された鍵を発生する機能を備え、

前記復号変換手段は、入力された前記鍵を、前記タイミング信号に合わせて前記更新された鍵に切り換える手段を備えたことを特徴とする請求の範囲第２６項記載のディジタル信号再生装置。

３０．前記再生手段は、前記ブロックの記録情報信号領域に記録されているところの、前記タイミングを識別可能な情報を、再生する機能を備えたことを特徴とする請求の範囲第２９項記載のディジタル信号再生装置。

３１．前記再生手段は、前記ブロックの付加情報信号領域に記録されているところの、前記タイミングを識別可能な情報を、再生する機能を備えたことを特徴とする請求の範囲第２９項記載のディジタル信号再生装置。

３２．前記再生手段は、前記ディジタル信号の各パケットに付加されて記録されているところの、前記タイミングを識別可能な情報を、再生する機能を備えたことを特徴とする請求の範囲第２９項記載のディジタル信号再生装置。

３３．前記再生手段は、前記第２の誤り訂正符号を付加したｎトラックの単位の区切り目で更新されているところの、前記鍵情報を、再生していく機能を備えたことを特徴とする請求の範囲第２９項記載のディジタル信号再生装置。

３４．前記再生手段は、前記記録媒体上の所定の領域に記録されている、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を再生する機能を備え、

前記復号変換手段は、前記暗号フラグ情報により、再生された前記ディジタル信号を復号化して出力する機能と、復号化しないでそのまま出

力する機能とを選択して切り換える機能を備えたことを特徴とする請求の範囲第２６項記載のディジタル信号再生装置。

３５．前記再生手段は、前記ブロックの記録情報信号領域に記録されているところの、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を、再生する機能を備えたことを特徴とする請求の範囲第３４項記載のディジタル信号再生装置。

３６．前記再生手段は、前記ブロックの付加情報信号領域に記録されているところの、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を、再生する機能を備えたことを特徴とする請求の範囲第３４項記載のディジタル信号再生装置。

３７．前記再生手段は、前記ディジタル信号の各パケットに付加して記録されているところの、前記ディジタル信号が暗号化されているか否か示す暗号フラグ情報を、再生する機能を備えたことを特徴とする請求の範囲第３４項記載のディジタル信号再生装置。

３８．前記再生手段は、前記第２の誤り訂正符号を付加したｎトラックの単位の区切り目で切り換えられているところの、前記暗号フラグを、再生していく機能を備えたことを特徴とする請求の範囲第３４項記載のディジタル信号再生装置。

３９．ディジタル信号が記録されているディジタル信号記録媒体において、

鍵情報に所定の演算を行って得られた鍵で暗号化された前記ディジタル信号と共に、前記鍵情報が、所定の領域に記録されていることを特徴とするディジタル信号記録媒体。

４０．前記ディジタル信号は、所定長のパケット形式を有してなることを特徴とする請求の範囲第３９項記載のディジタル信号記録媒体。

４１．前記鍵情報が所定間隔で更新され、所定の領域に記録されている

ことを特徴とする請求の範囲第３９項記載のディジタル信号記録媒体。

４２．前記鍵情報が所定間隔で更新されたことを示すタイミングを識別可能な情報が、所定の領域に記録されていることを特徴とする請求の範囲第３９項記載のディジタル信号記録媒体。

４３．前記ディジタル信号が暗号化されているか否かを示す暗号フラグ情報が、所定の領域に記録されていて、前記ディジタル信号が暗号化されていない場合は、前記鍵情報は記録されていないこと特徴とする請求の範囲第３９項記載のディジタル信号記録媒体。

４４．ディジタル信号を変換するための複数種類の鍵を発生する鍵発生手段と、

前記鍵を用いてディジタル信号を変換し、変換後の変換ディジタル信号を出力する変換手段と、

前記鍵および前記変換ディジタル信号を記録媒体に記録する記録手段と、

を備えてなることを特徴とするディジタル信号記録装置。

４５．複数種類の鍵で変換された変換ディジタル信号および前記鍵が記録された媒体が用いられ、

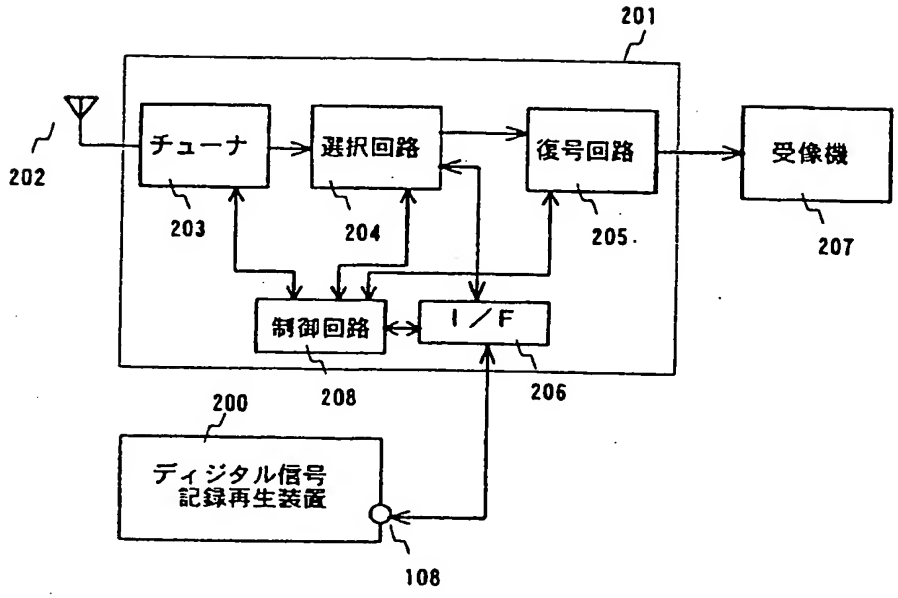
前記変換ディジタル信号および前記鍵を前記媒体から再生し、出力する再生手段と、

前記再生手段からの出力が入力され、前記変換ディジタル信号を前記鍵を用いて復号変換する復号変換手段と、

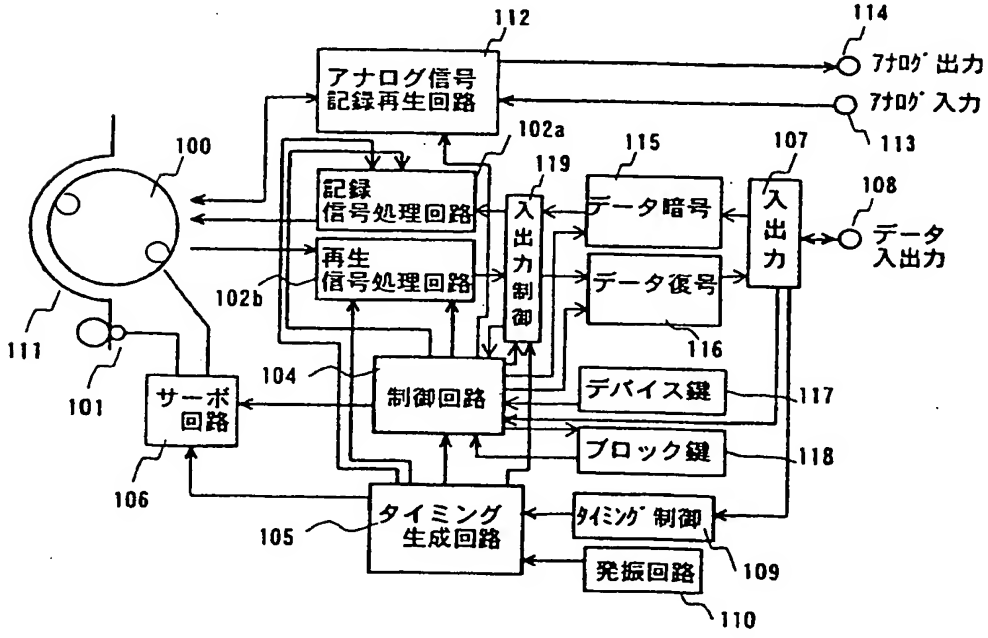
を備えてなるディジタル信号再生装置

４６．複数種類の鍵で変換された変換ディジタル信号および前記鍵が記録された記録媒体。

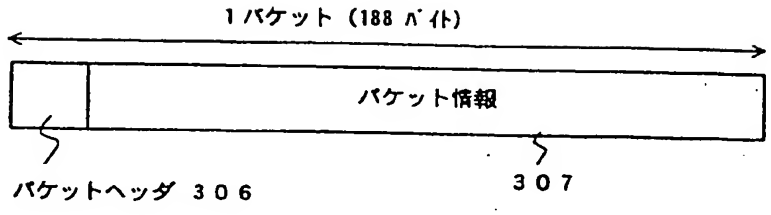
第1図


201
202
チューナ
選択回路
復号回路
受像機
203
204
205
207
制御回路
I/F
208
206
200
ディジタル信号
記録再生装置
108

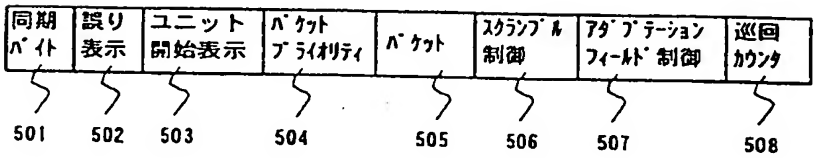
第2図


112
114
アナログ信号
記録再生回路
ｱﾅﾛｸﾞ出力
ｱﾅﾛｸﾞ入力
113
102a
115
107
100
119
108
記録
信号処理回路
入出力制御
データ暗号
入出力
データ
入出力
再生
信号処理回路
102b
データ復号
116
111
101
104
制御回路
デバイス鍵
117
サーボ
回路
ブロック鍵
118
106
タイミング
生成回路
105
ﾀｲﾐﾝｸﾞ制御
109
発振回路
110

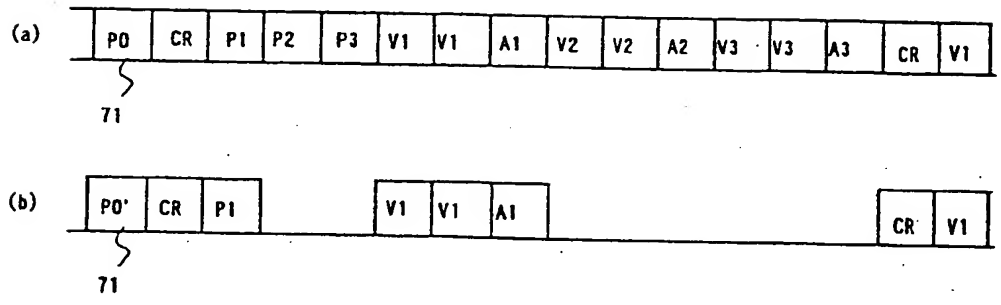
第3図


1パケット（188バイト）
パケット情報
パケットヘッダ 306
307

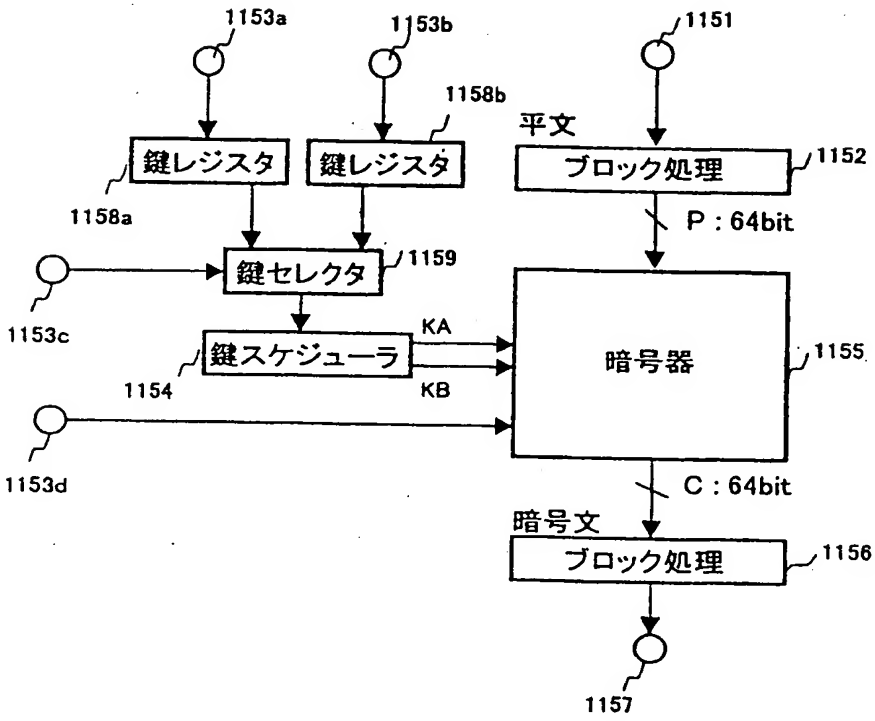
第4図


同期バイト
誤り表示
ユニット開始表示
パケットプライオリティ
パケット
スクランブル制御
アダプテーションフィールド制御
巡回カウンタ
501
502
503
504
505
506
507
508

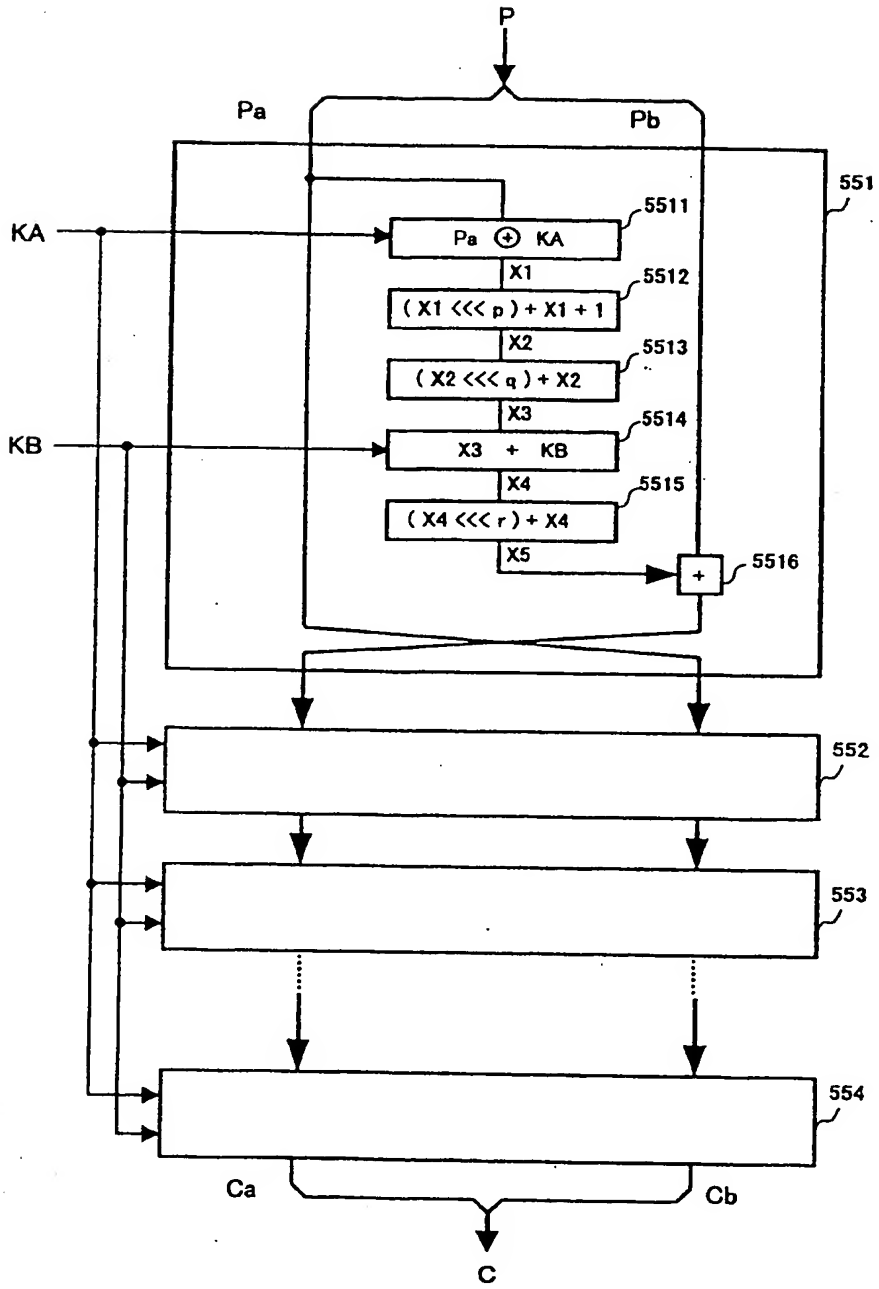
第5図


(a)
P0 CR P1 P2 P3 V1 V1 A1 V2 V2 A2 V3 V3 A3 CR V1
71
(b)
P0' CR P1 V1 V1 A1 CR V1
71

第6図

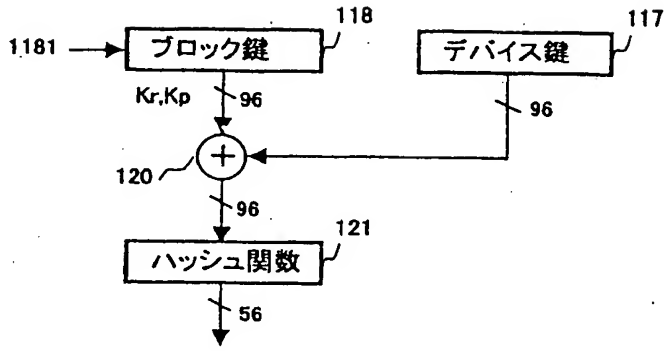

1153a
1153b
1151
1158b
平文
鍵レジスタ
鍵レジスタ
ブロック処理
1152
1158a
P : 64bit
鍵セレクタ
1159
1153c
KA
鍵スケジューラ
暗号器
1155
1154
KB
1153d
C : 64bit
暗号文
ブロック処理
1156
1157

第7図

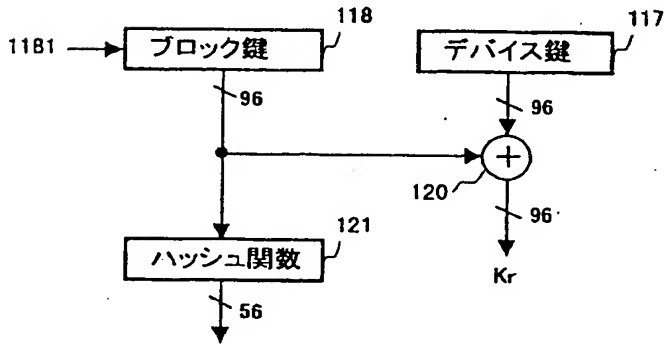

P
Pa
Pb
551
KA
5511
Pa ⊕ KA
X1
5512
(X1 <<< p) + X1 + 1
X2
5513
(X2 <<< q) + X2
X3
KB
5514
X3 + KB
X4
5515
(X4 <<< r) + X4
X5
5516
+
552
553
554
Ca
Cb
C

第8図

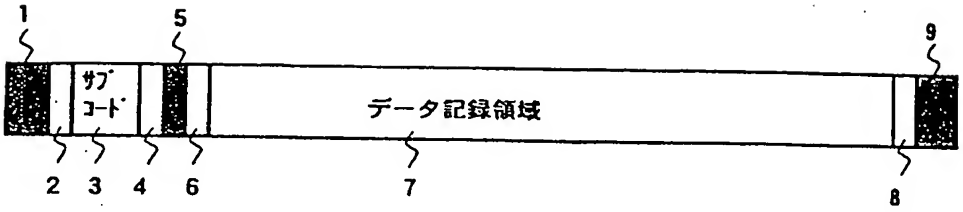
(a)


1181
ブロック鍵
118
デバイス鍵
117
Kr,Kp
96
96
120
96
ハッシュ関数
121
56

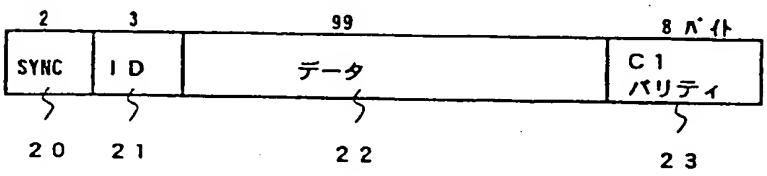
(b)


1181
ブロック鍵
118
デバイス鍵
117
96
96
120
96
ハッシュ関数
121
Kr
56

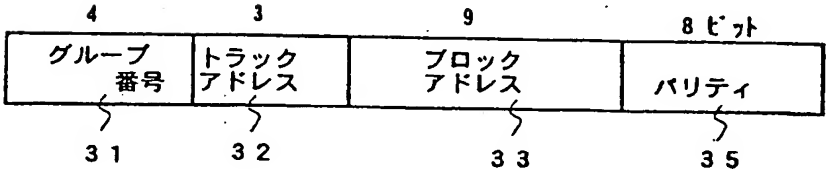
第９図



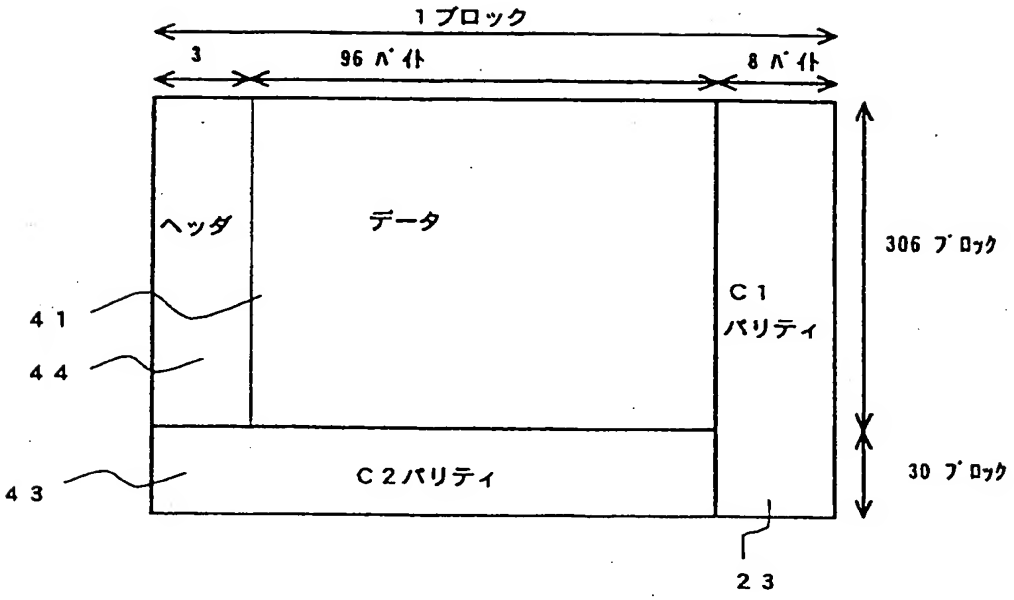
第１０図



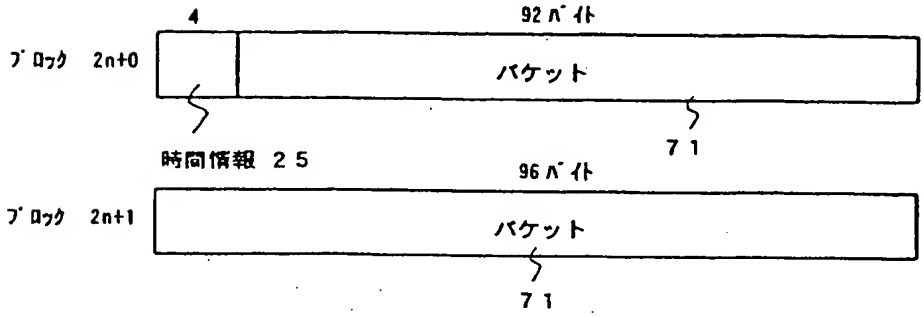
第１１図



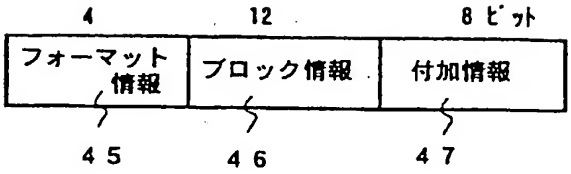
第１２図


1ブロック
3
96 バイト
8 バイト
ヘッダ
データ
C1
パリティ
306 ブロック
41
44
C2パリティ
30 ブロック
43
23

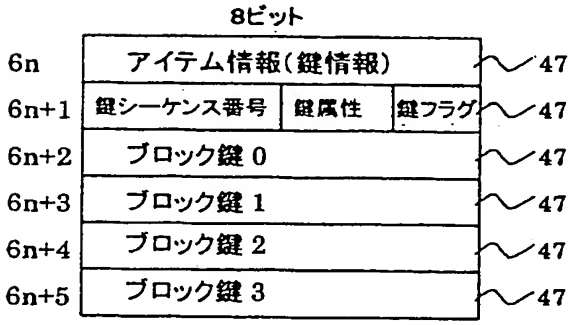
第１３図


4
92 バイト
ブロック 2n+0
パケット
71
時間情報 25
96 バイト
ブロック 2n+1
パケット
71

第１４図


4
12
8 ビット
フォーマット情報
ブロック情報
付加情報
45
46
47

第１５図


8ビット
6n
アイテム情報(鍵情報)
47
6n+1
鍵シーケンス番号
鍵属性
鍵フラグ
47
6n+2
ブロック鍵 0
47
6n+3
ブロック鍵 1
47
6n+4
ブロック鍵 2
47
6n+5
ブロック鍵 3
47

第16図

(1)

6a	"鍵情報"		
6a+1	"2"	"0"	"0"
6a+2	ブロック鍵 A0		
6a+3	ブロック鍵 A1		
6a+4	ブロック鍵 A2		
6a+5	ブロック鍵 A3		

6b	"鍵情報"		
6b+1	"1"	"0"	"0"
6b+2	ブロック鍵 A4		
6b+3	ブロック鍵 A5		
6b+4	ブロック鍵 A6		
6b+5	ブロック鍵 A7		

6c	"鍵情報"		
6c+1	"0"	"0"	"0"
6c+2	ブロック鍵 A8		
6c+3	ブロック鍵 A9		
6c+4	ブロック鍵 A10		
6c+5	ブロック鍵 A11		

(2)

6d	"鍵情報"		
6d+1	"2"	"0"	"1"
6d+2	ブロック鍵 B0		
6d+3	ブロック鍵 B1		
6d+4	ブロック鍵 B2		
6d+5	ブロック鍵 B3		

6e	"鍵情報"		
6e+1	"1"	"0"	"1"
6e+2	ブロック鍵 B4		
6e+3	ブロック鍵 B5		
6e+4	ブロック鍵 B6		
6e+5	ブロック鍵 B7		

6f	"鍵情報"		
6f+1	"0"	"0"	"1"
6f+2	ブロック鍵 B8		
6f+3	ブロック鍵 B9		
6f+4	ブロック鍵 B10		
6f+5	ブロック鍵 B11		

第17図

(1)

6a	"鍵情報"		
6a+1	"2"	"0"	"0"
6a+2	ブロック鍵 A0		
6a+3	ブロック鍵 A1		
6a+4	ブロック鍵 A2		
6a+5	ブロック鍵 A3		

6b	"鍵情報"		
6b+1	"1"	"0"	"0"
6b+2	ブロック鍵 A4		
6b+3	ブロック鍵 A5		
6b+4	ブロック鍵 A6		
6b+5	ブロック鍵 A7		

6c	"鍵情報"		
6c+1	"0"	"0"	"0"
6c+2	ブロック鍵 A8		
6c+3	ブロック鍵 A9		
6c+4	ブロック鍵 A10		
6c+5	ブロック鍵 A11		

(2)

6d	"鍵情報"		
6d+1	"2"	"1"	"1"
6d+2	ブロック鍵 B0		
6d+3	ブロック鍵 B1		
6d+4	ブロック鍵 B2		
6d+5	ブロック鍵 B3		

6e	"鍵情報"		
6e+1	"1"	"1"	"1"
6e+2	ブロック鍵 B4		
6e+3	ブロック鍵 B5		
6e+4	ブロック鍵 B6		
6e+5	ブロック鍵 B7		

6f	"鍵情報"		
6f+1	"0"	"1"	"1"
6f+2	ブロック鍵 B8		
6f+3	ブロック鍵 B9		
6f+4	ブロック鍵 B10		
6f+5	ブロック鍵 B11		

(3)

6a	"鍵情報"		
6a+1	"2"	"0"	"1"
6a+2	ブロック鍵 B0		
6a+3	ブロック鍵 B1		
6a+4	ブロック鍵 B2		
6a+5	ブロック鍵 B3		

6b	"鍵情報"		
6b+1	"1"	"0"	"1"
6b+2	ブロック鍵 B4		
6b+3	ブロック鍵 B5		
6b+4	ブロック鍵 B6		
6b+5	ブロック鍵 B7		

6c	"鍵情報"		
6c+1	"0"	"0"	"1"
6c+2	ブロック鍵 B8		
6c+3	ブロック鍵 B9		
6c+4	ブロック鍵 B10		
6c+5	ブロック鍵 B11		

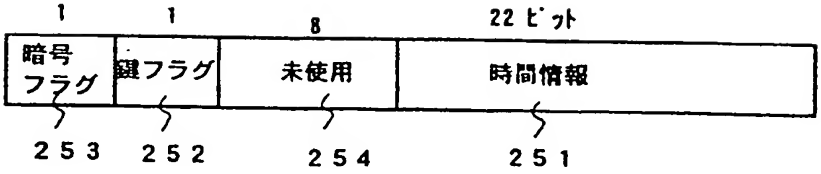
(4)

6d	"鍵情報"		
6d+1	"2"	"1"	"0"
6d+2	ブロック鍵 C0		
6d+3	ブロック鍵 C1		
6d+4	ブロック鍵 C2		
6d+5	ブロック鍵 C3		

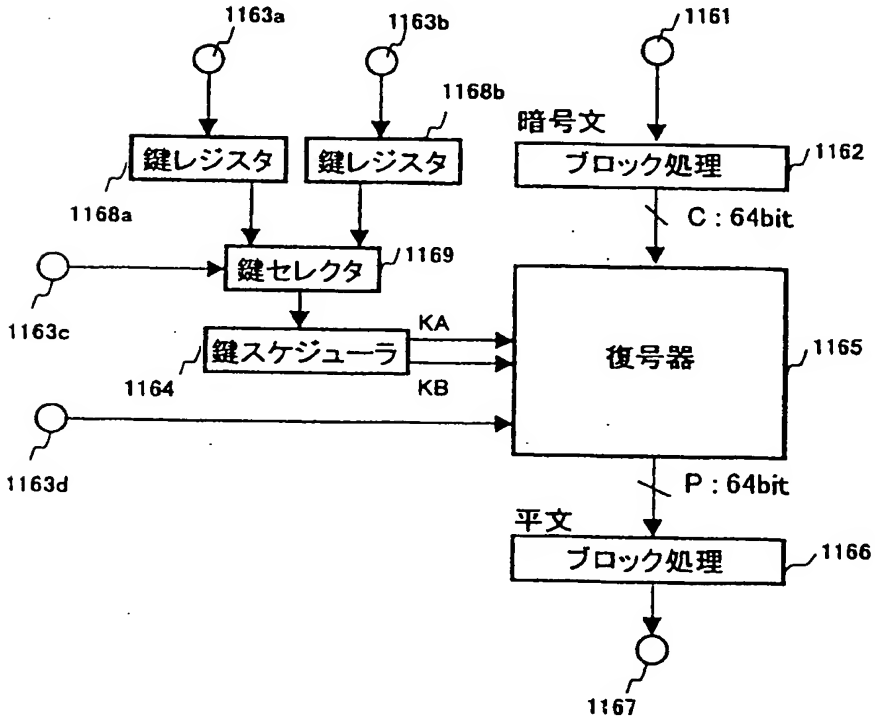
6e	"鍵情報"		
6e+1	"1"	"1"	"0"
6e+2	ブロック鍵 C4		
6e+3	ブロック鍵 C5		
6e+4	ブロック鍵 C6		
6e+5	ブロック鍵 C7		

6f	"鍵情報"		
6f+1	"0"	"0"	"0"
6f+2	ブロック鍵 C8		
6f+3	ブロック鍵 C9		
6f+4	ブロック鍵 C10		
6f+5	ブロック鍵 C11		

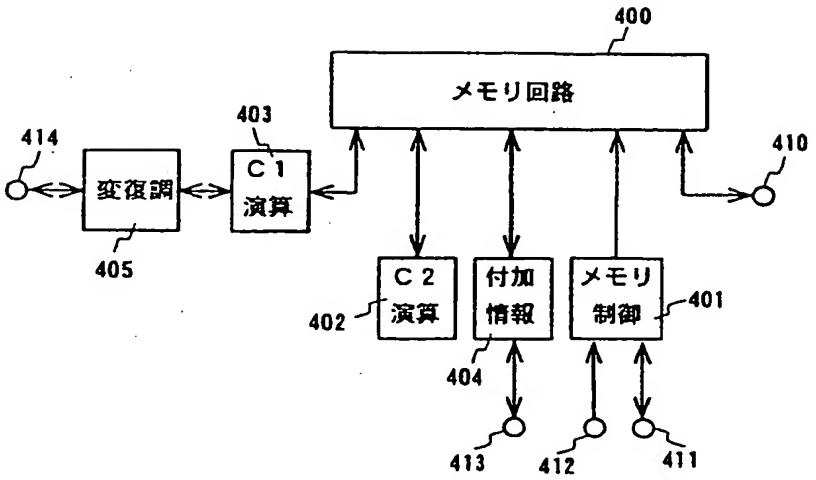
第１８図


1
1
8
22 ビット
暗号フラグ
鍵フラグ
未使用
時間情報
253
252
254
251

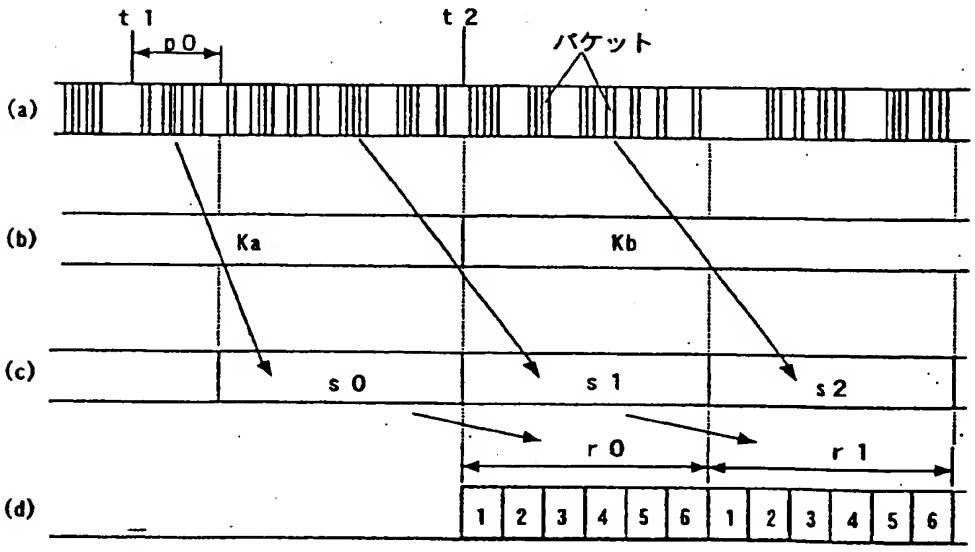
第１９図


1163a
1163b
1161
1168b
暗号文
鍵レジスタ
鍵レジスタ
ブロック処理
1162
1168a
C：64bit
鍵セレクタ
1169
1163c
KA
鍵スケジューラ
復号器
1165
1164
KB
1163d
P：64bit
平文
ブロック処理
1166
1167

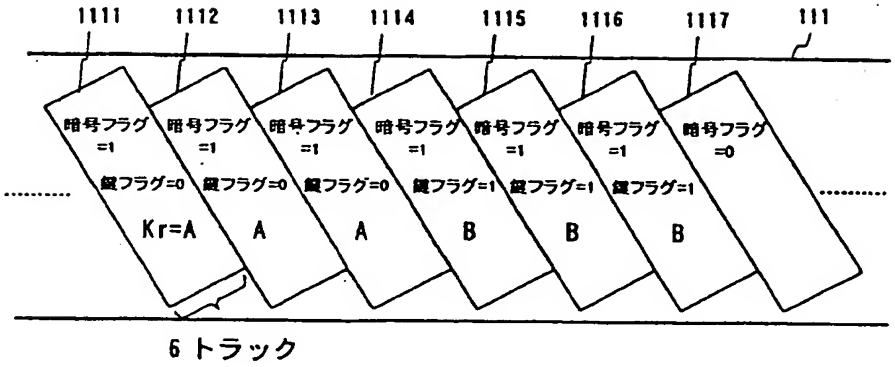
第２０図


400
メモリ回路
403
414
変復調
C 1
演算
410
405
C 2
演算
付加
情報
メモリ
制御
402
401
404
413
412
411

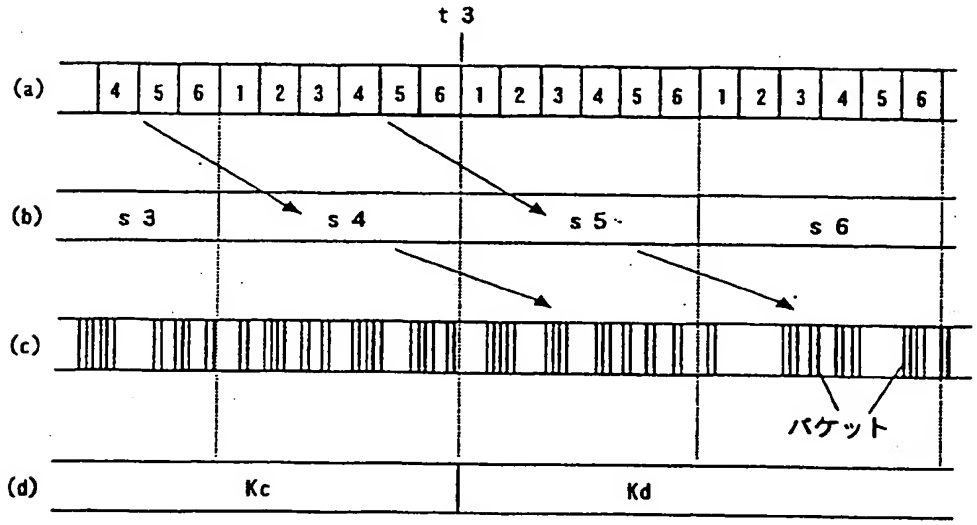
第２１図


t 1
p 0
t 2
パケット
(a)
(b)
Ka
Kb
(c)
s 0
s 1
s 2
r 0
r 1
(d)
1 2 3 4 5 6 1 2 3 4 5 6

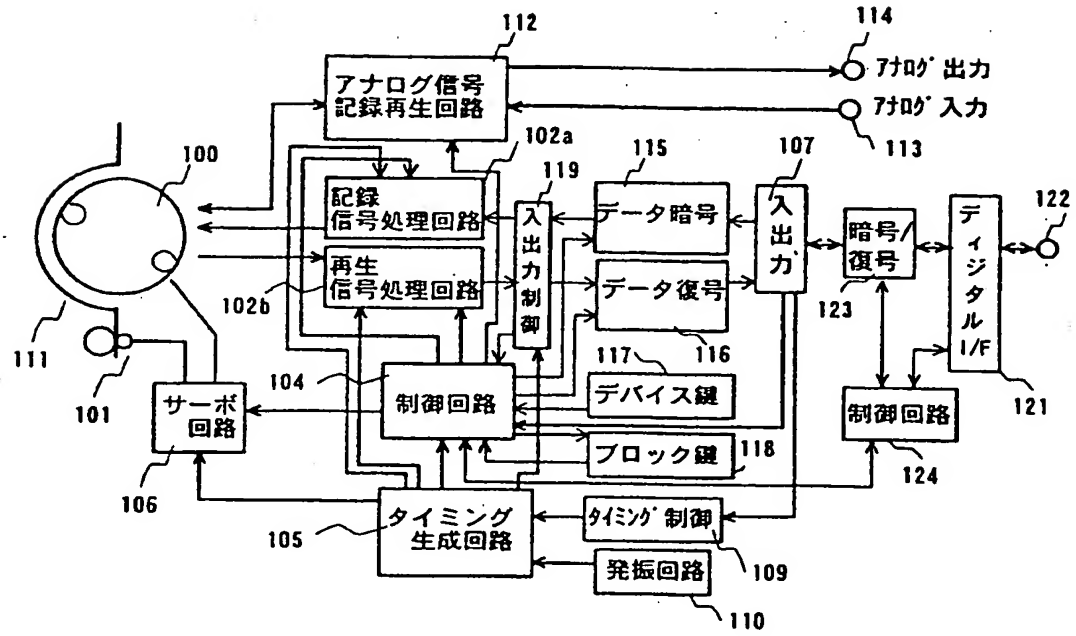
第２２図


1111
1112
1113
1114
1115
1116
1117
111
暗号フラグ=1
鍵フラグ=0
Kr=A
A
A
暗号フラグ=1
鍵フラグ=1
B
B
暗号フラグ=1
鍵フラグ=1
B
暗号フラグ=0
6トラック

第２３図


t3
(a)
4 5 6 1 2 3 4 5 6 1 2 3 4 5 6 1 2 3 4 5 6
(b)
s3
s4
s5
s6
(c)
パケット
(d)
Kc
Kd

第２４図


112
114
アナログ信号
記録再生回路
ｱﾅﾛｸﾞ出力
ｱﾅﾛｸﾞ入力
113
100
102a
119
115
107
記録
信号処理回路
データ暗号
入出力
暗号/
復号
ディジタル
I/F
122
再生
信号処理回路
入出力制御
データ復号
102b
123
111
117
116
104
デバイス鍵
101
サーボ
回路
制御回路
制御回路
121
ブロック鍵
118
124
106
タイミング
生成回路
ﾀｲﾐﾝｸﾞ制御
105
109
発振回路
110

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/00929

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] G11B20/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] G11B20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-1999
Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 6-231536, A (Matsushita Electric Industrial Co., Ltd.), 19 August, 1994 (19. 08. 94), Full text ; Figs. 1, 2 (Family: none)	1-46
A	JP, 7-288798, A (Mitsubishi Electric Corp.), 31 October, 1995 (31. 10. 95), Full text ; Figs. 1 to 10 (Family: none)	1-46
A	JP, 9-214882, A (Victor Co. of Japan,Ltd.), 15 August, 1997 (15. 08. 97), Full text ; Figs. 1 to 5 (Family: none)	1-46
A	JP, 10-241287, A (Matsushita Electric Industrial Co., Ltd.), 11 September, 1998 (11. 09. 98), Full text ; Figs. 1 to 9 (Family: none)	1-46

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
24 May, 1999 (24. 05. 99)

Date of mailing of the international search report
1 June, 1999 (01. 06. 99)

Name and mailing address of the ISA/
Japanese Patent Office

Facsimile No.

Authorized officer

Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号　PCT／JP99／00929

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl°　G11B20／10

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl°　G11B20／10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－1999年
日本国登録実用新案公報	1994－1999年
日本国実用新案登録公報	1996－1999年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP，6－231536，A（松下電器産業株式会社）19．8月．1994（19．08．94） 全文，第1－2図（ファミリーなし）	1－46
A	JP，7－288798，A（三菱電機株式会社）31．10月．1995（31．10．95） 全文，第1－10図（ファミリーなし）	1－46
A	JP，9－214882，A（日本ビクター株式会社）15．8月．1997（15．08．97） 全文，第1－5図（ファミリーなし）	1－46

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 24．05．99	国際調査報告の発送日　01.06.99
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 小松　正　印　SQ　7736 電話番号　03－3581－1101　内線　6922

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号 PCT／JP99／00929

C（続き）. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP, 10－241287, A (松下電器産業株式会社) 11. 9月. 1998 (11. 09. 98) 全文, 第1－9図 (ファミリーなし)	1－46